

# The Four Types of Locks

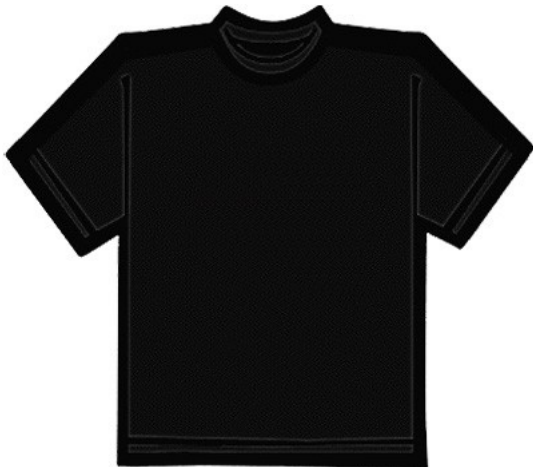


by Deviant Ollam  
Event Name  
XXXX-XX-XX

# Who am i ?



# Who am i ?

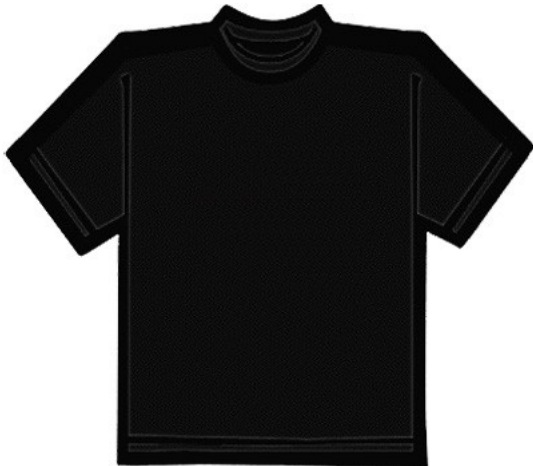


# Who am i ?



**THE  
CORE  
GROUP**

**auditing  
assessments  
research  
trainings**



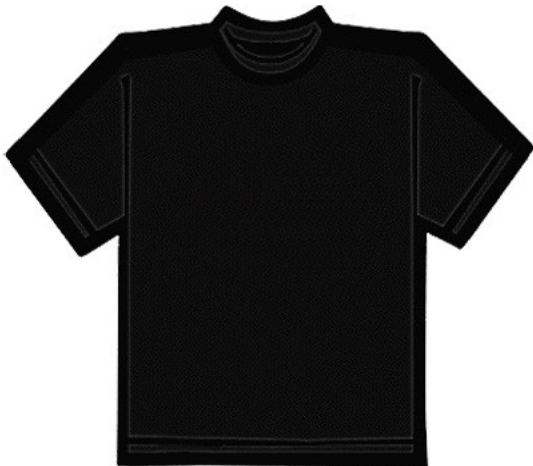


# Who am i ?



**THE  
CORE  
GROUP**

**auditing  
assessments  
research  
trainings**



**workshops  
public lectures  
lockpick village  
contests & games**

# Who am i ?



# Who am i ?





# Who am i ?



# But on to locks...



# But on to locks..... why do they matter?















# All your hard work here...

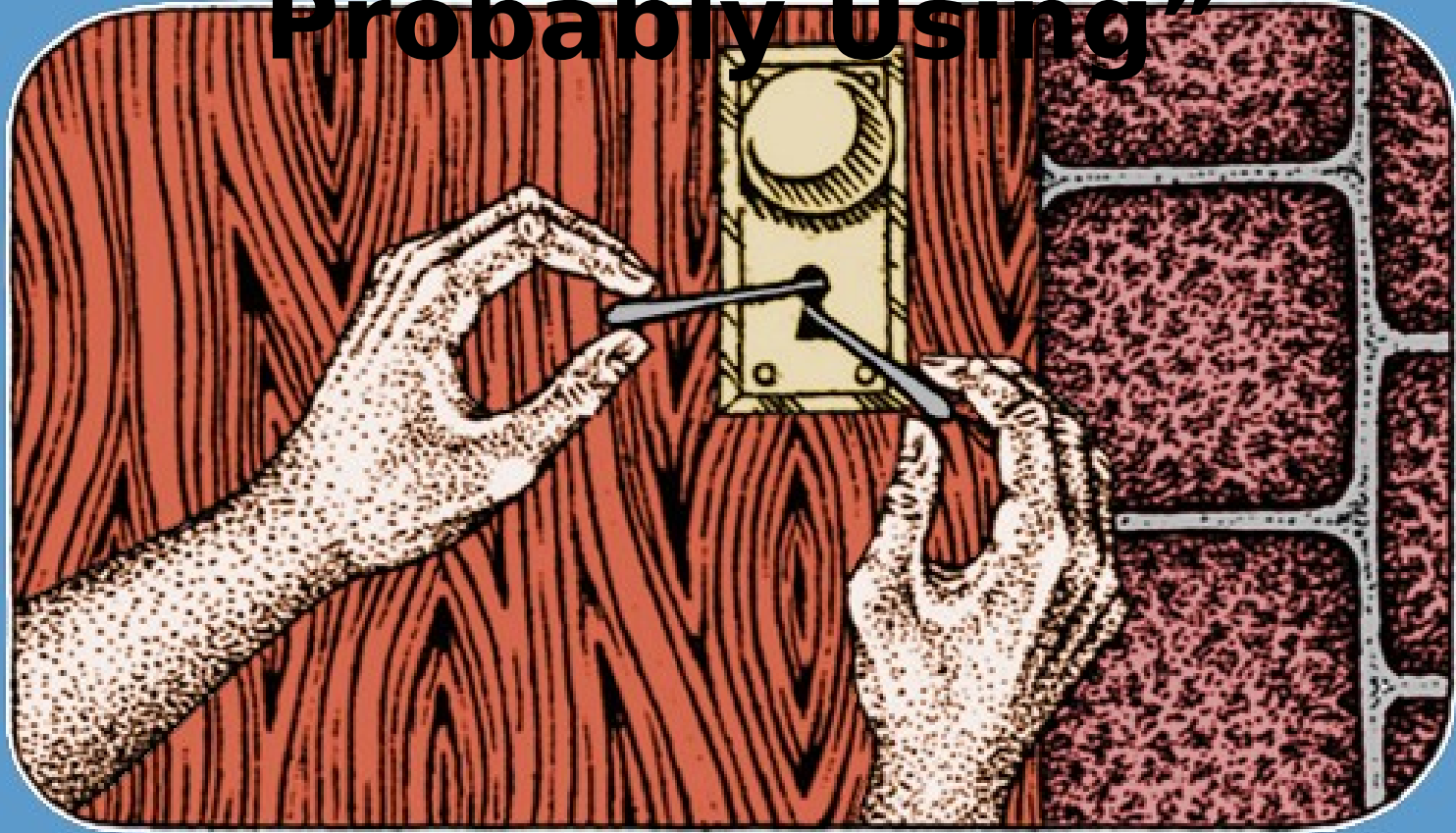


# All your hard work here...gets unlocked here





# The Lowest Grade of Lock... a.k.a. “The Locks That You Are Probably Using”



# Pin Tumbler Locks



# Pin Tumbler Locks

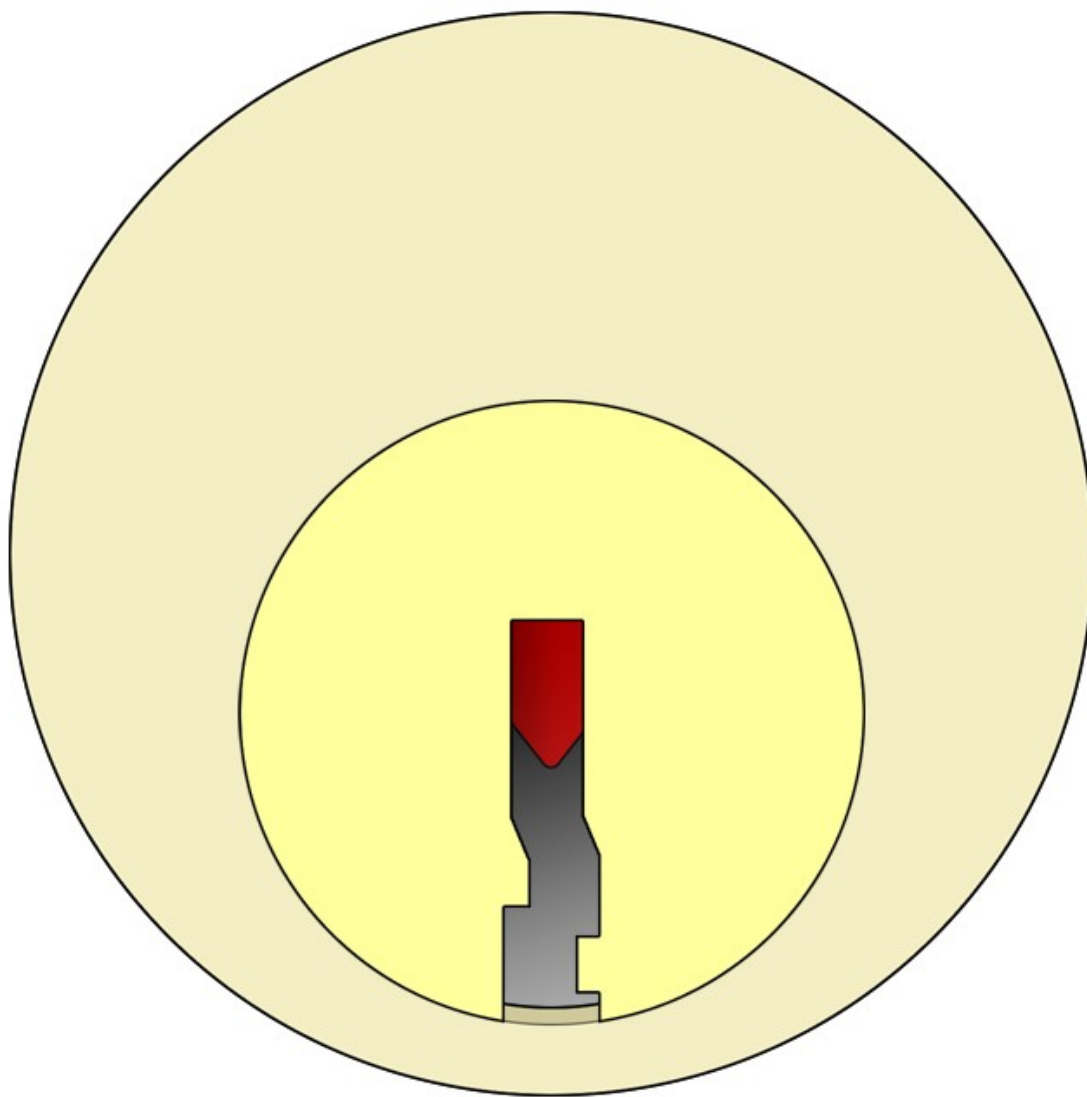


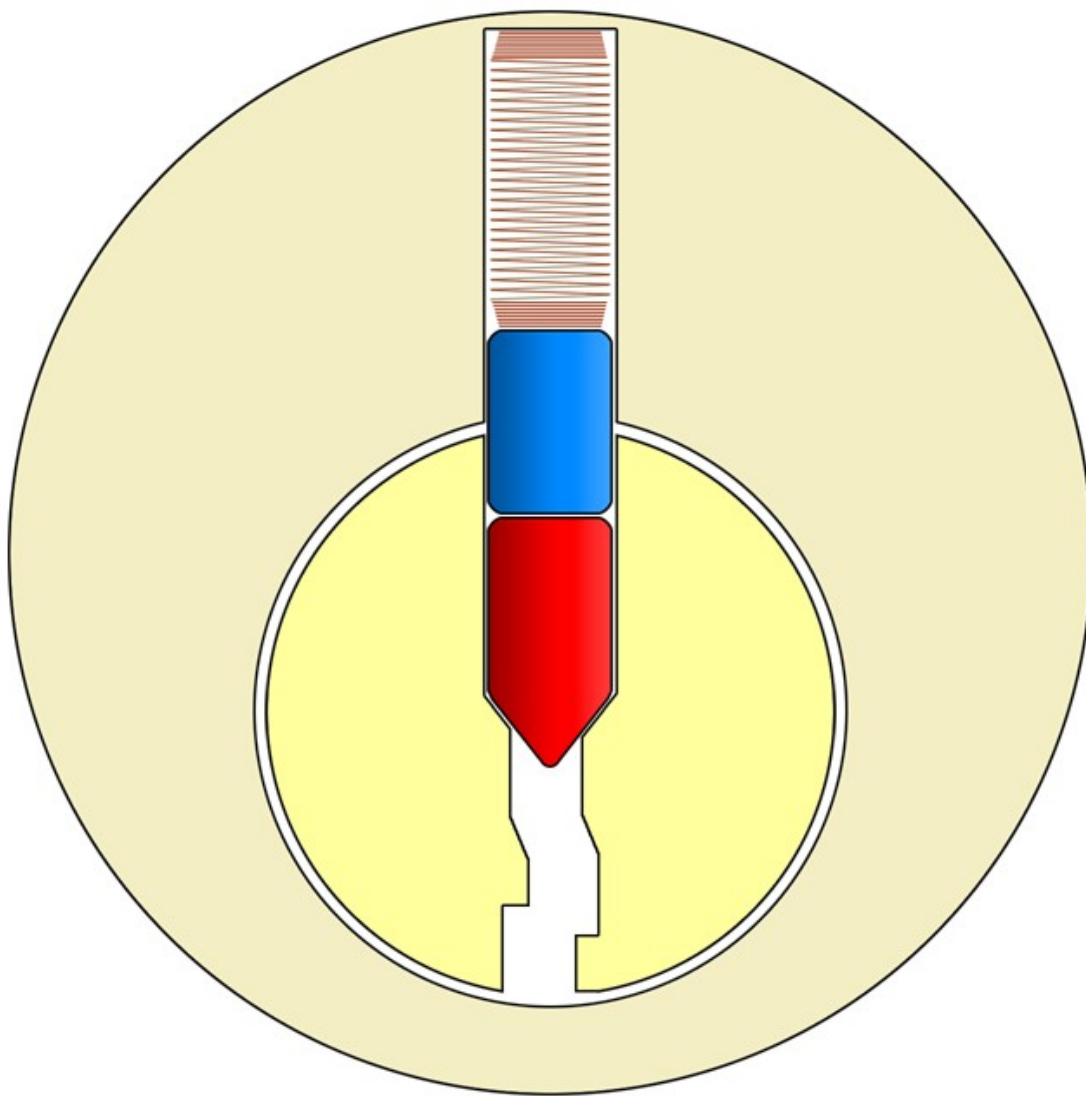


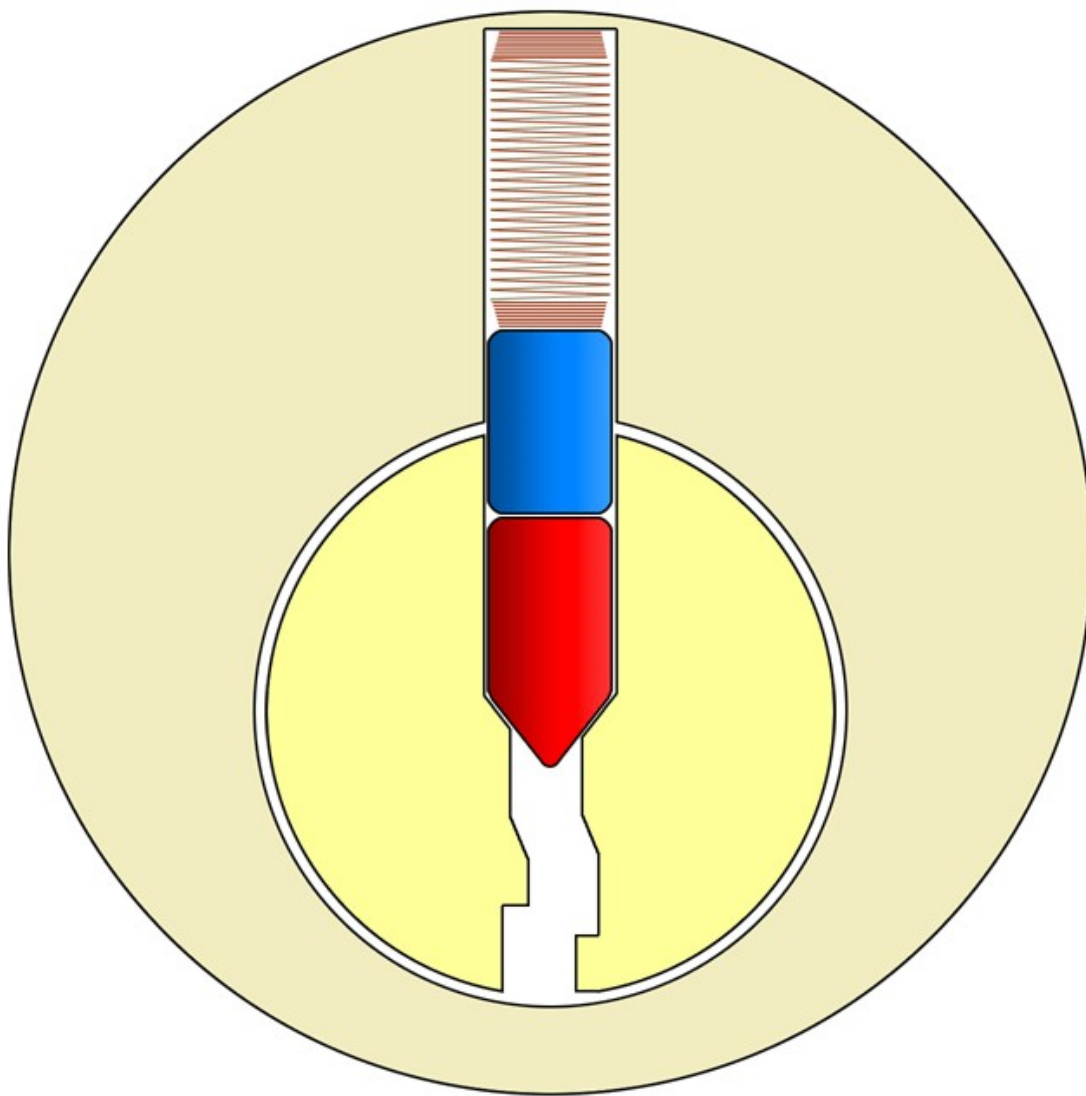
# Pin Tumbler Locks

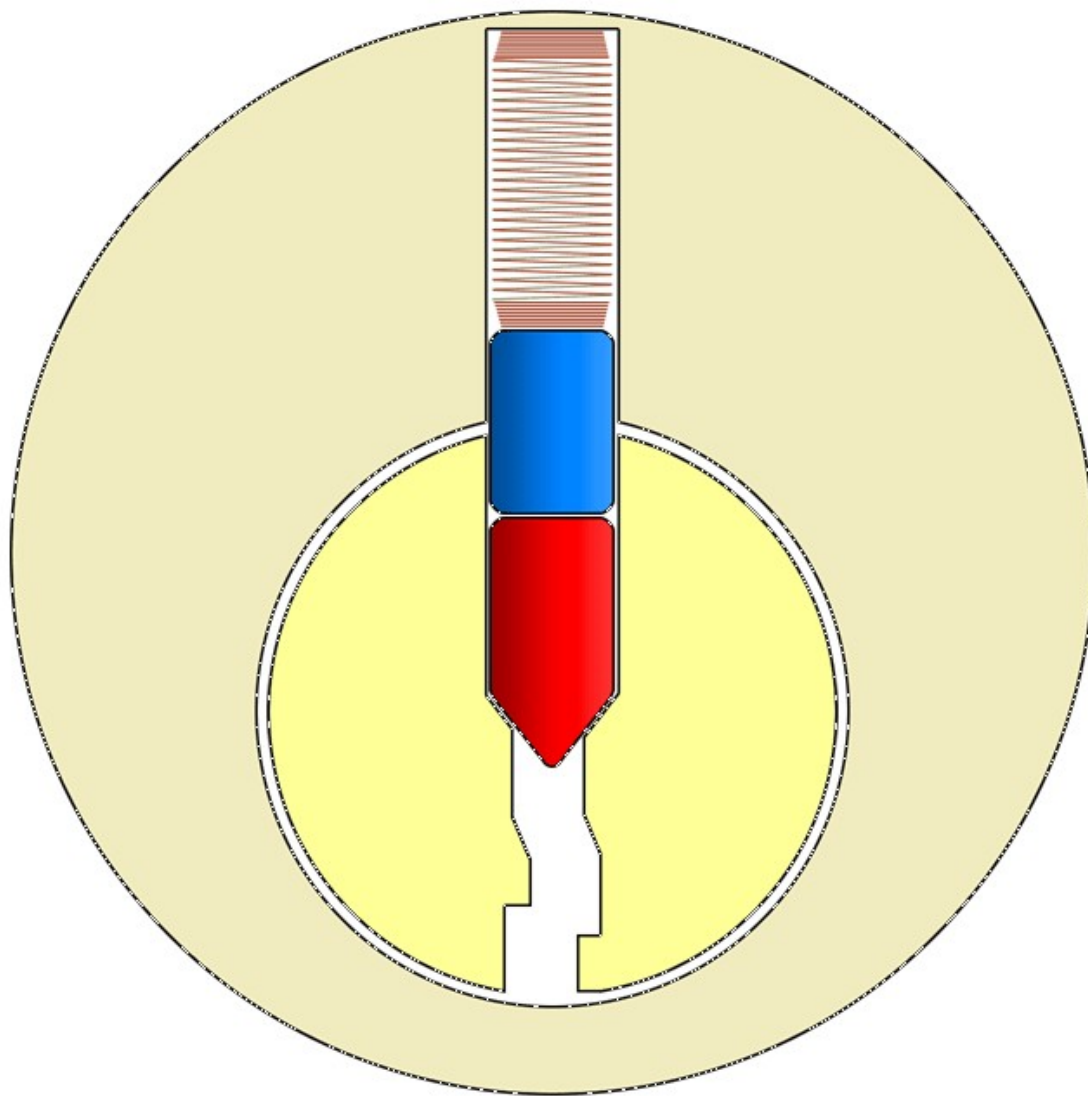




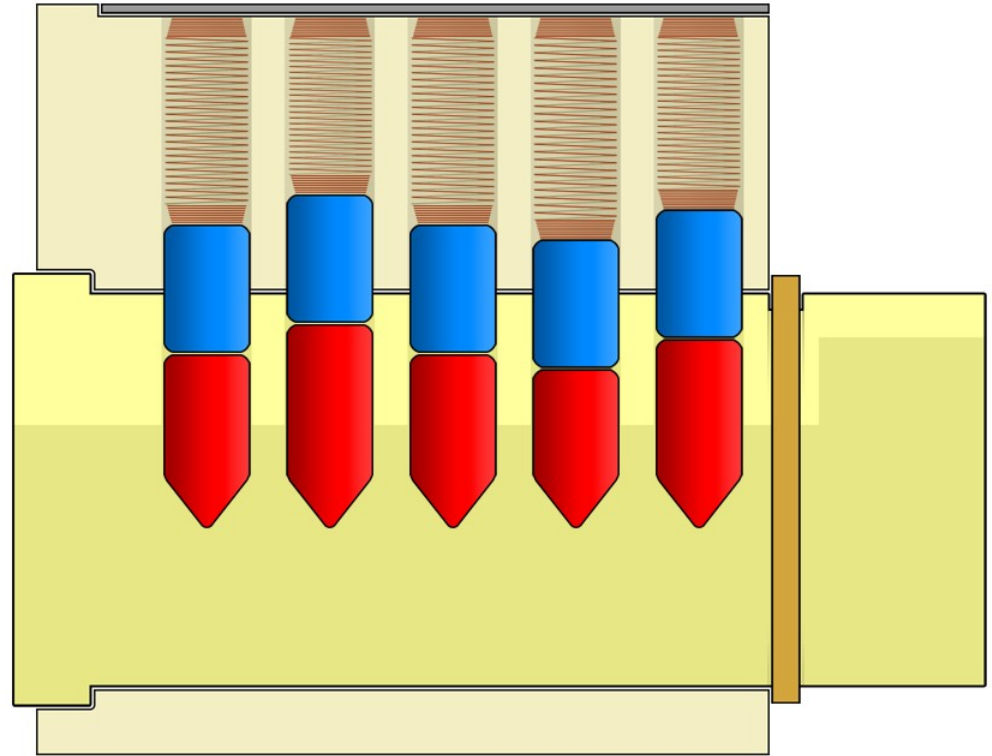




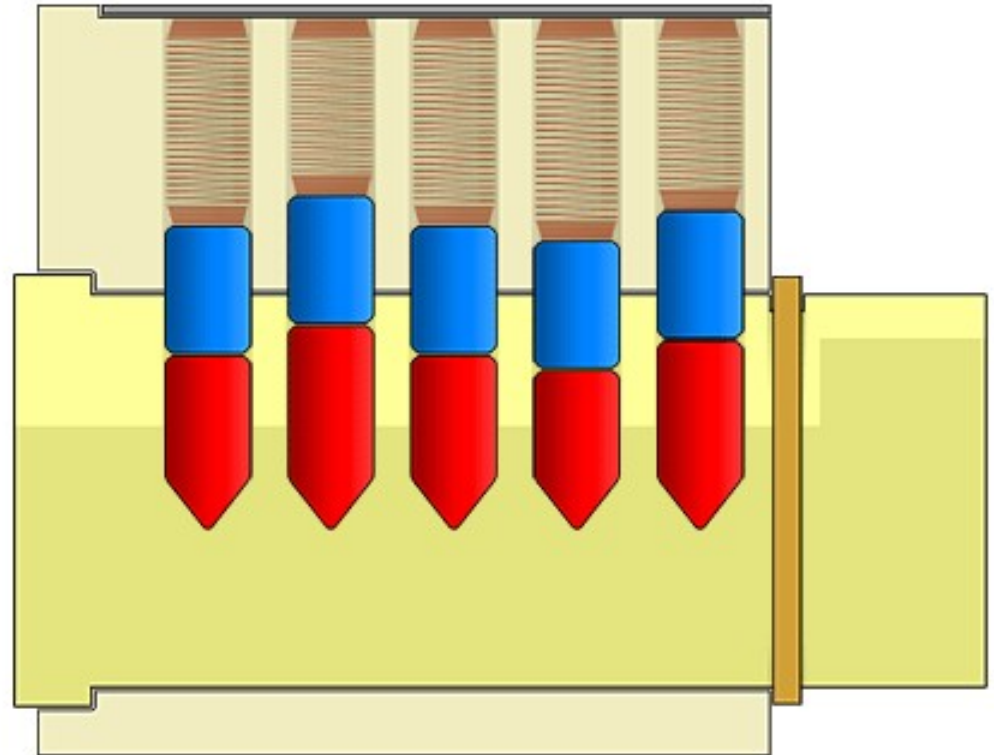




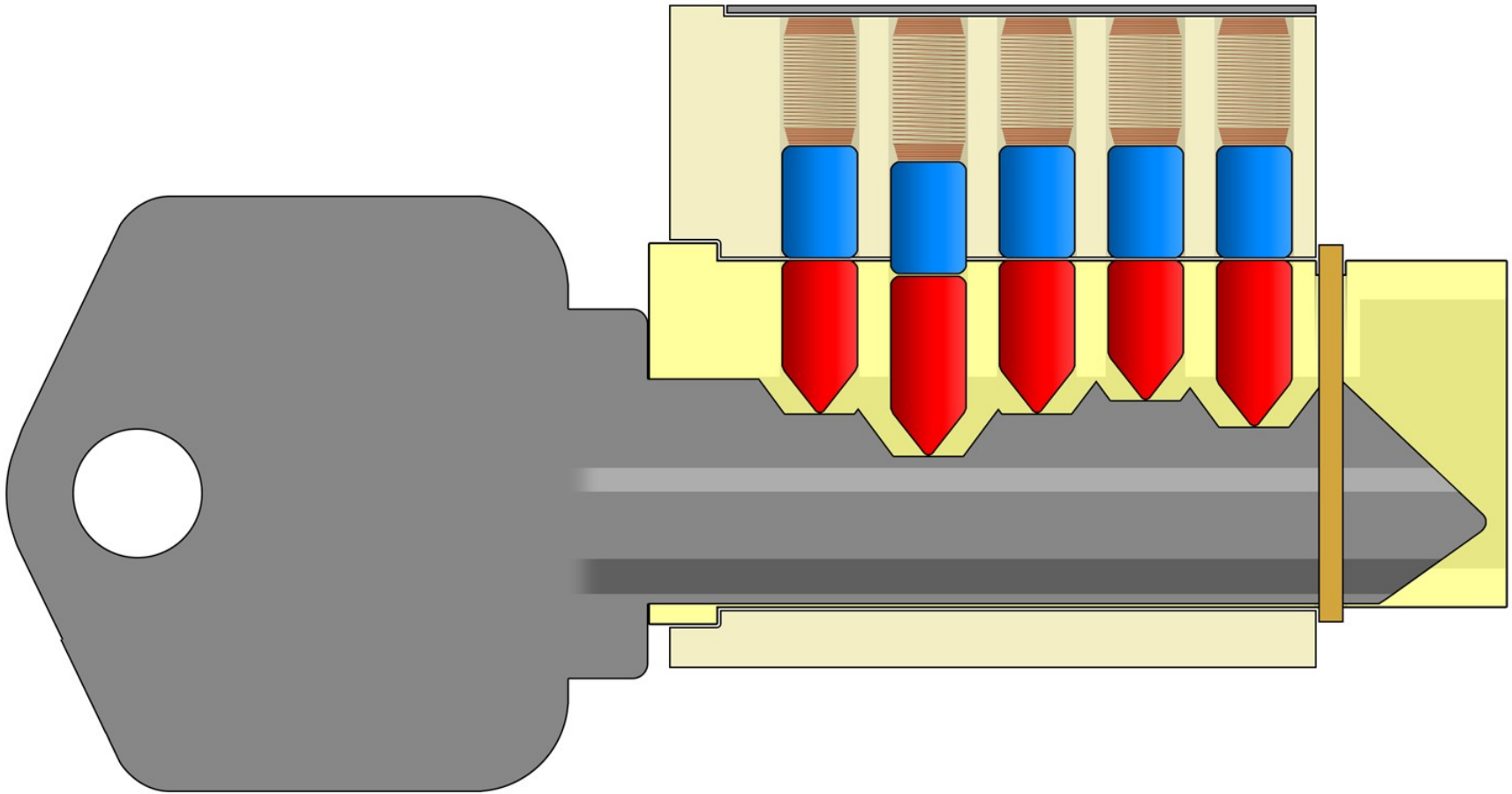
# Pin Stacks



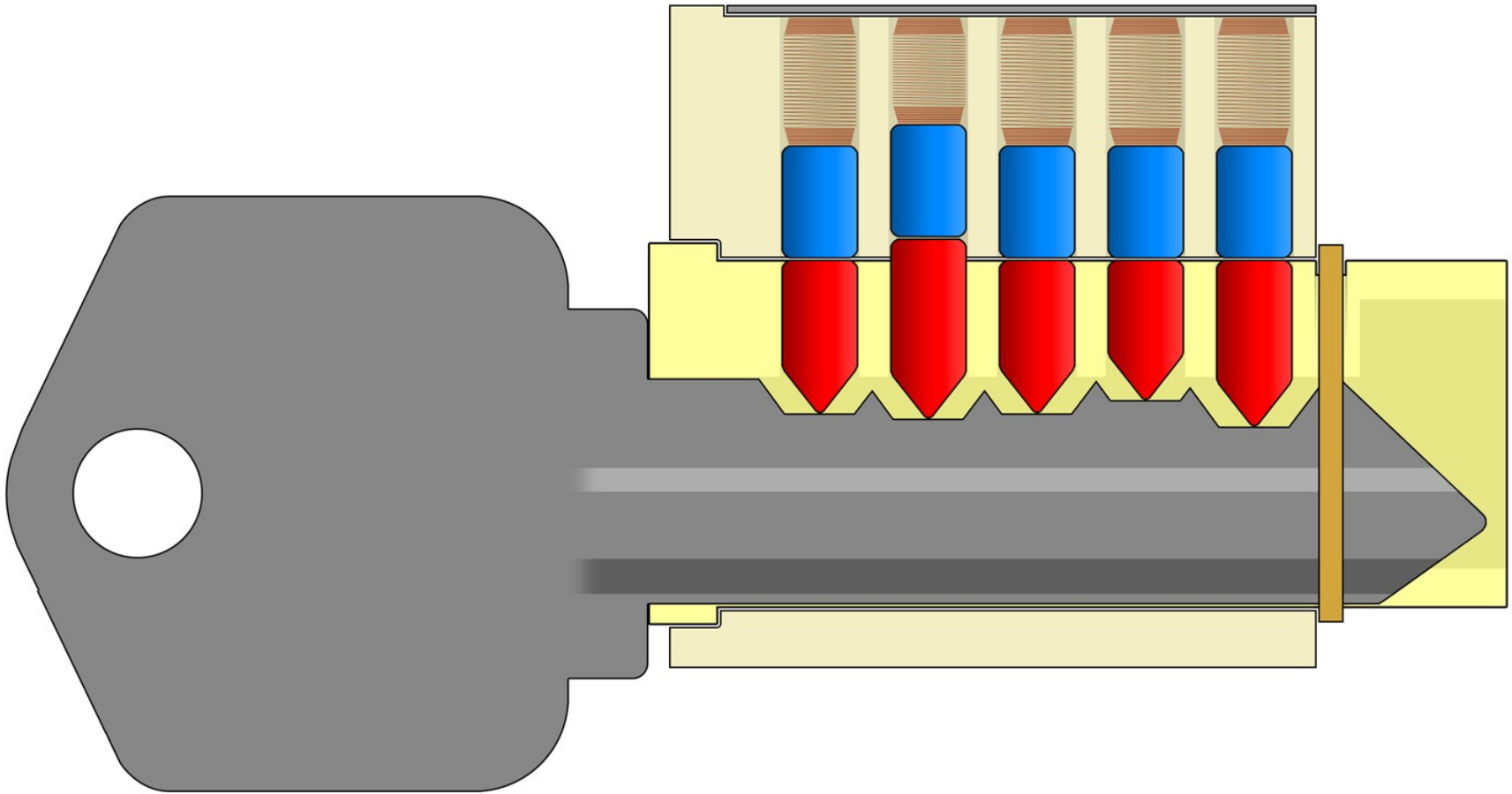
# Key Operation



# Bitting Too Low

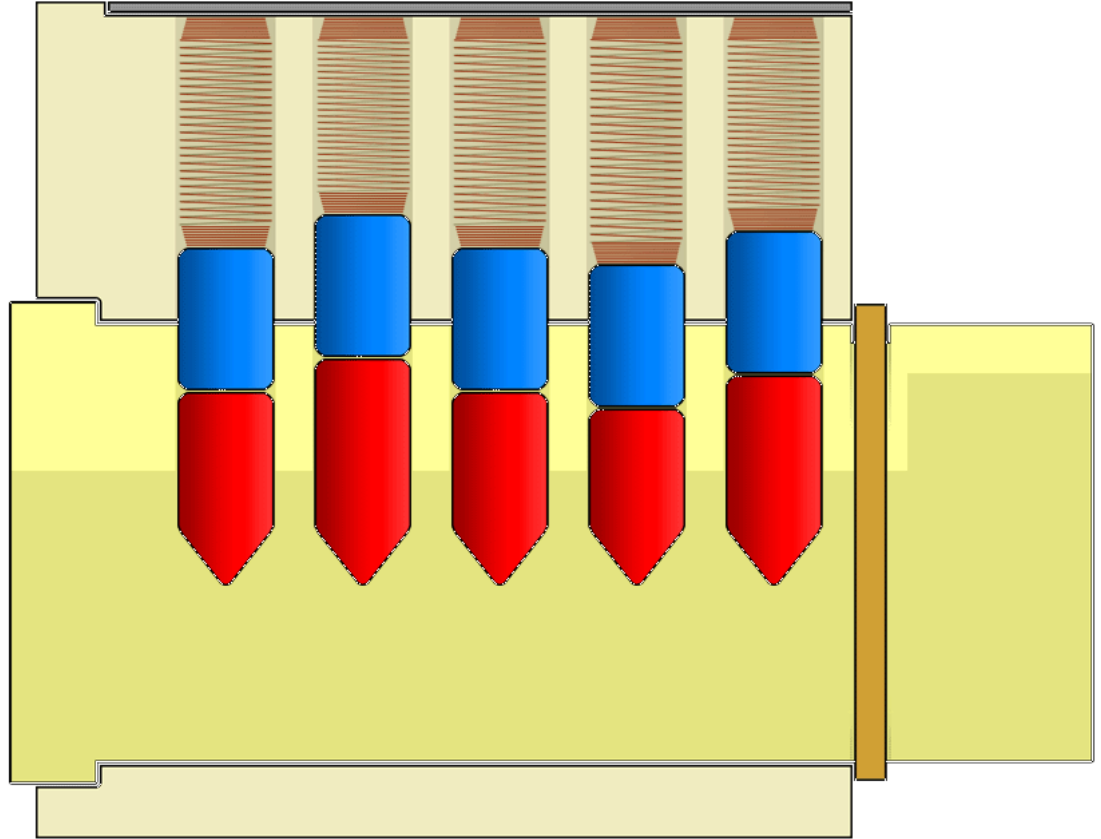
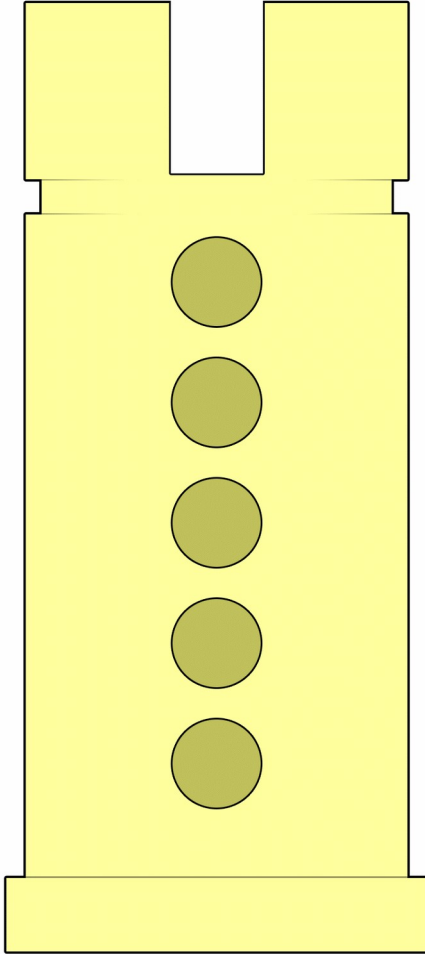


# Bitting Too High

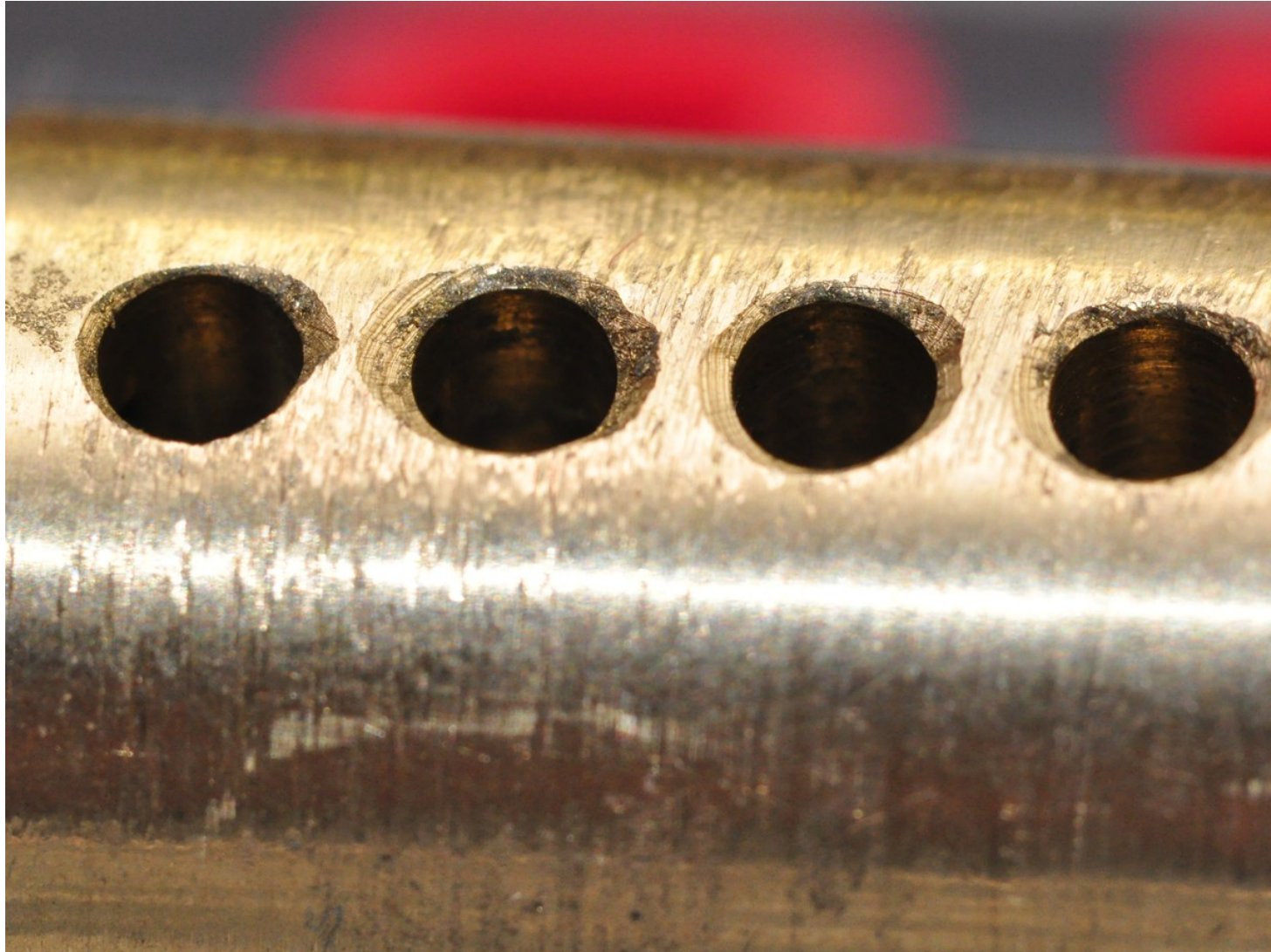




# In a Perfect World



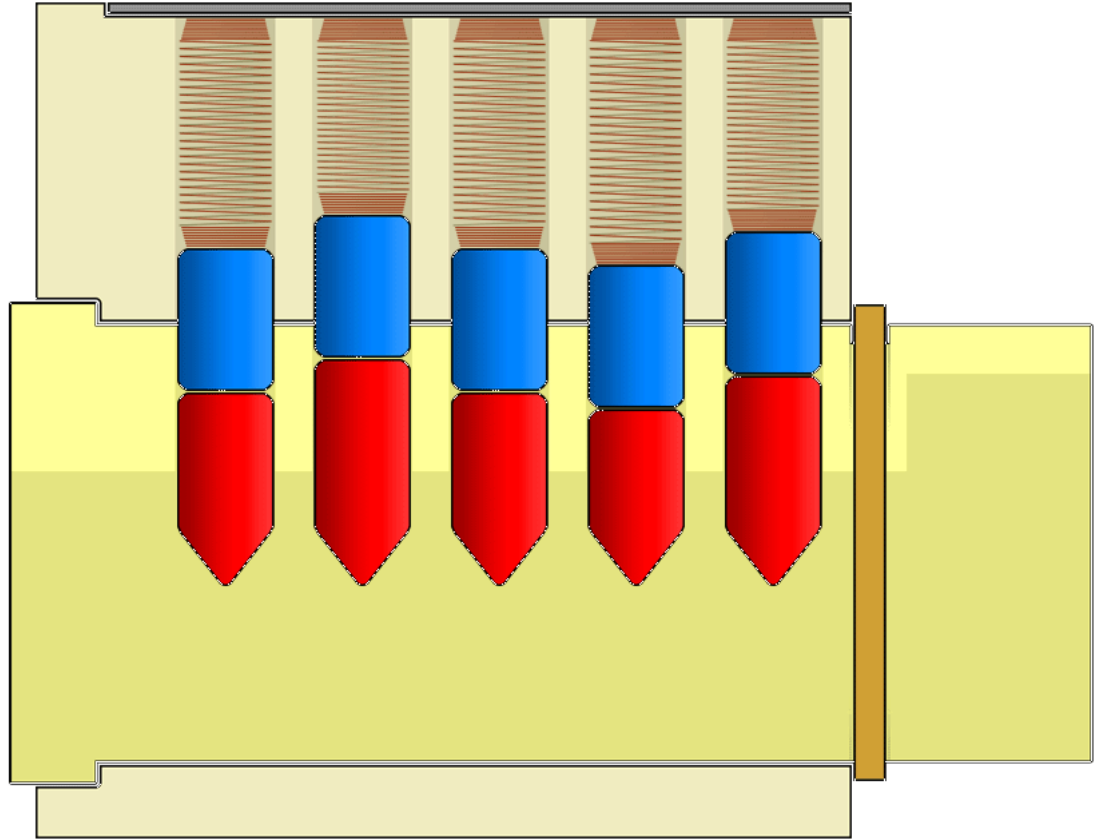
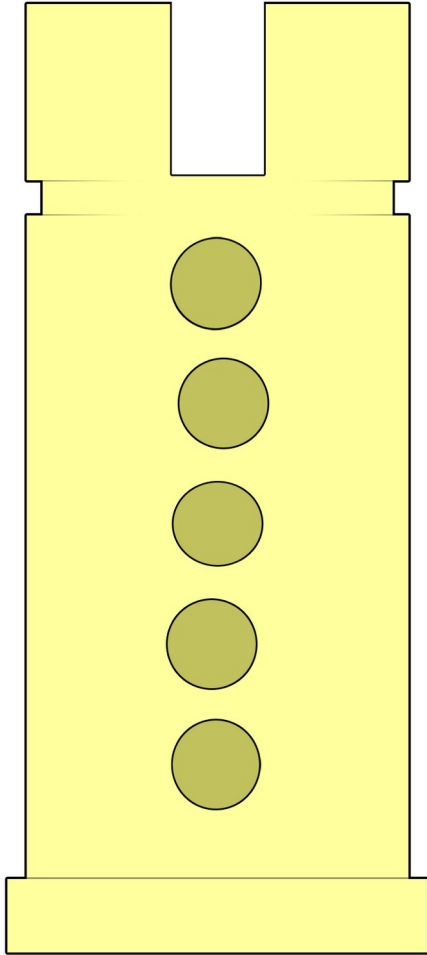
# In the Real World



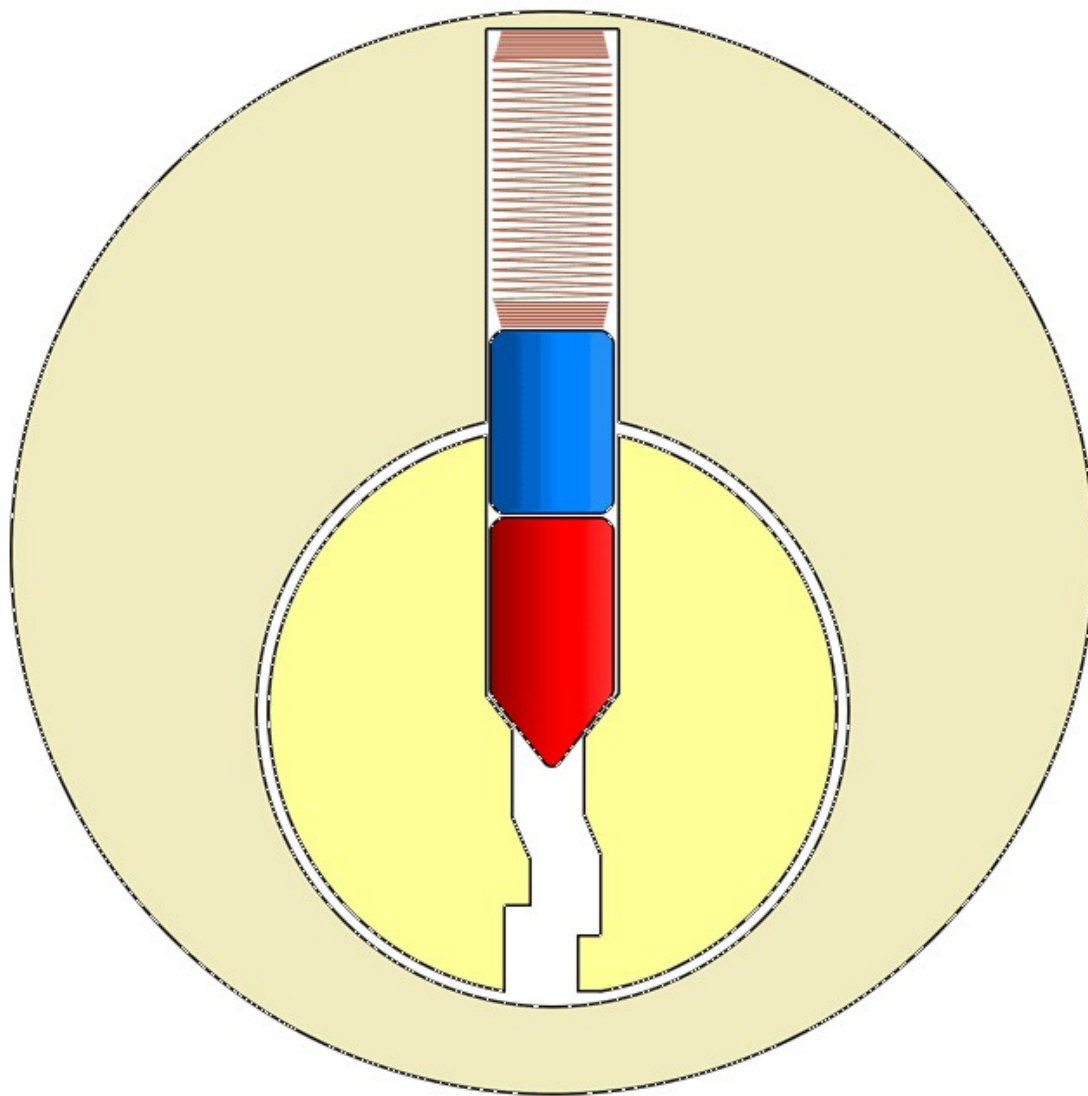
# In the Real World

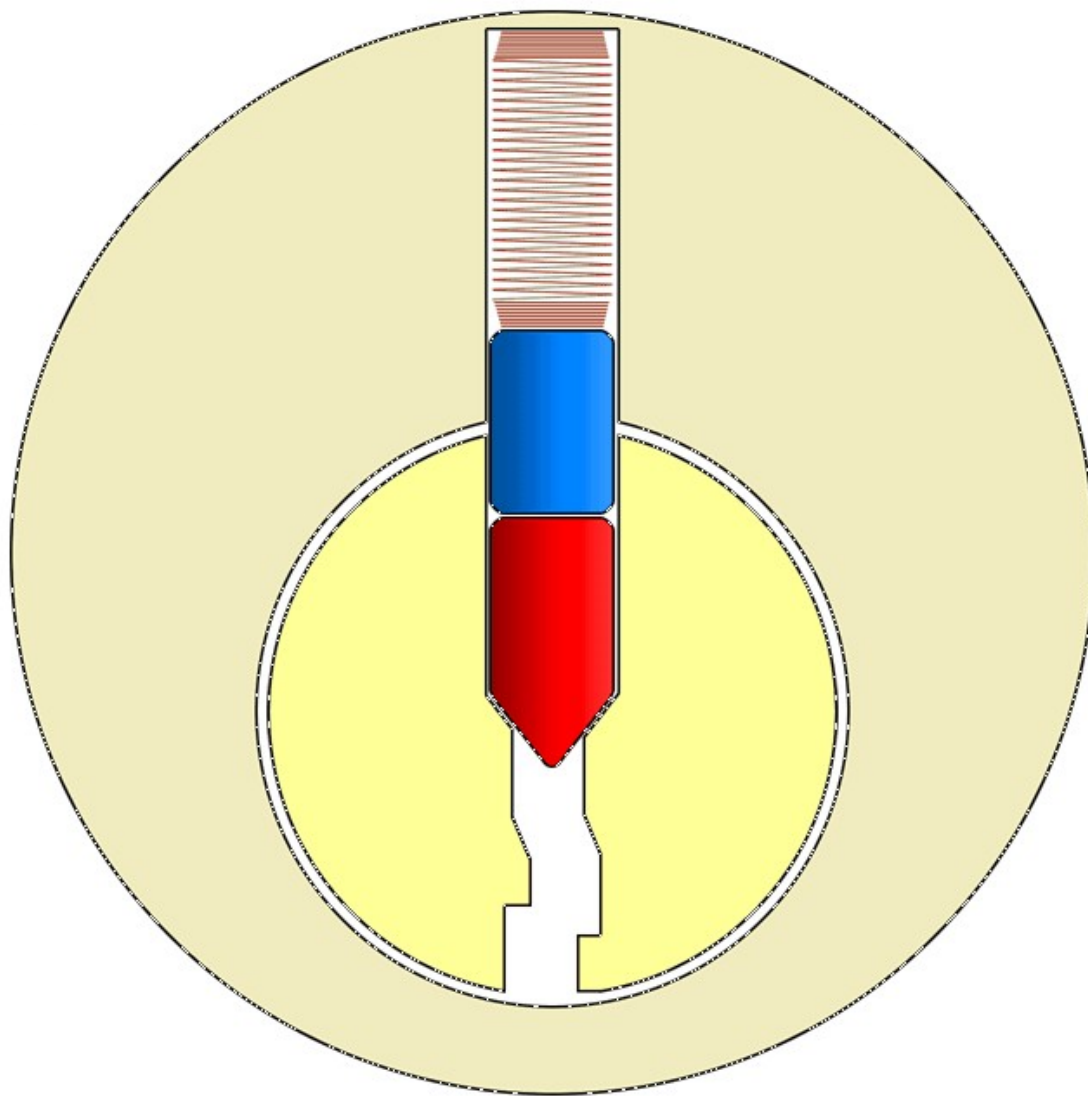


# In the Real World

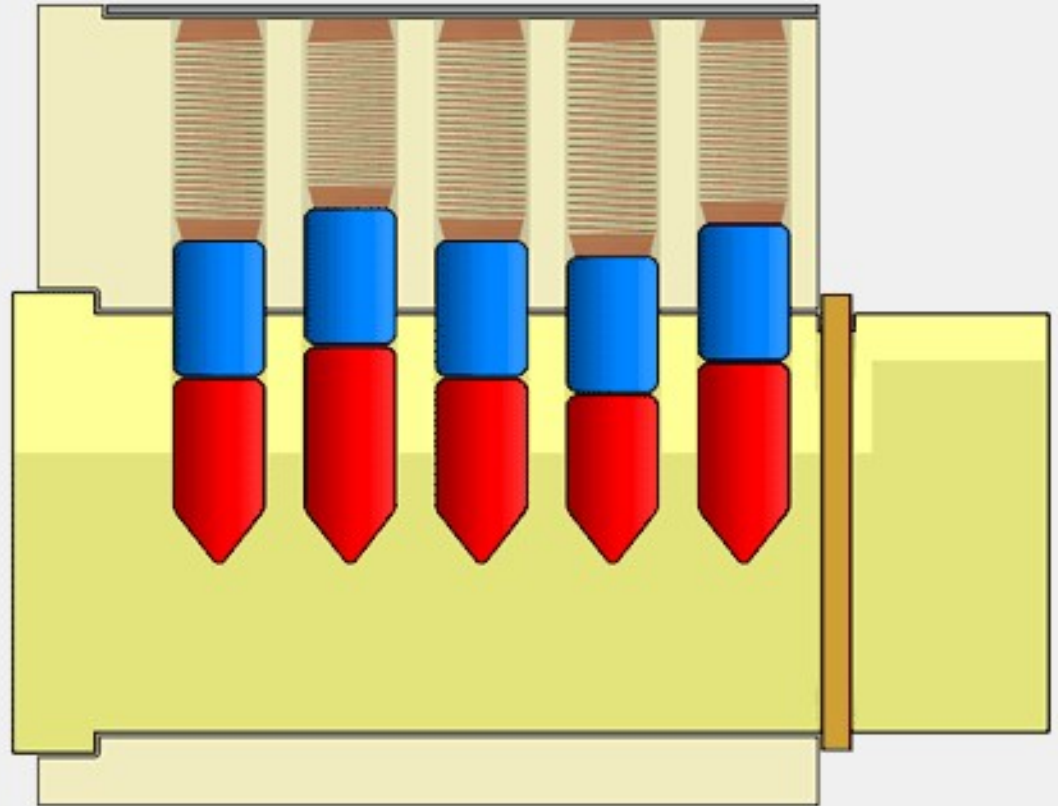




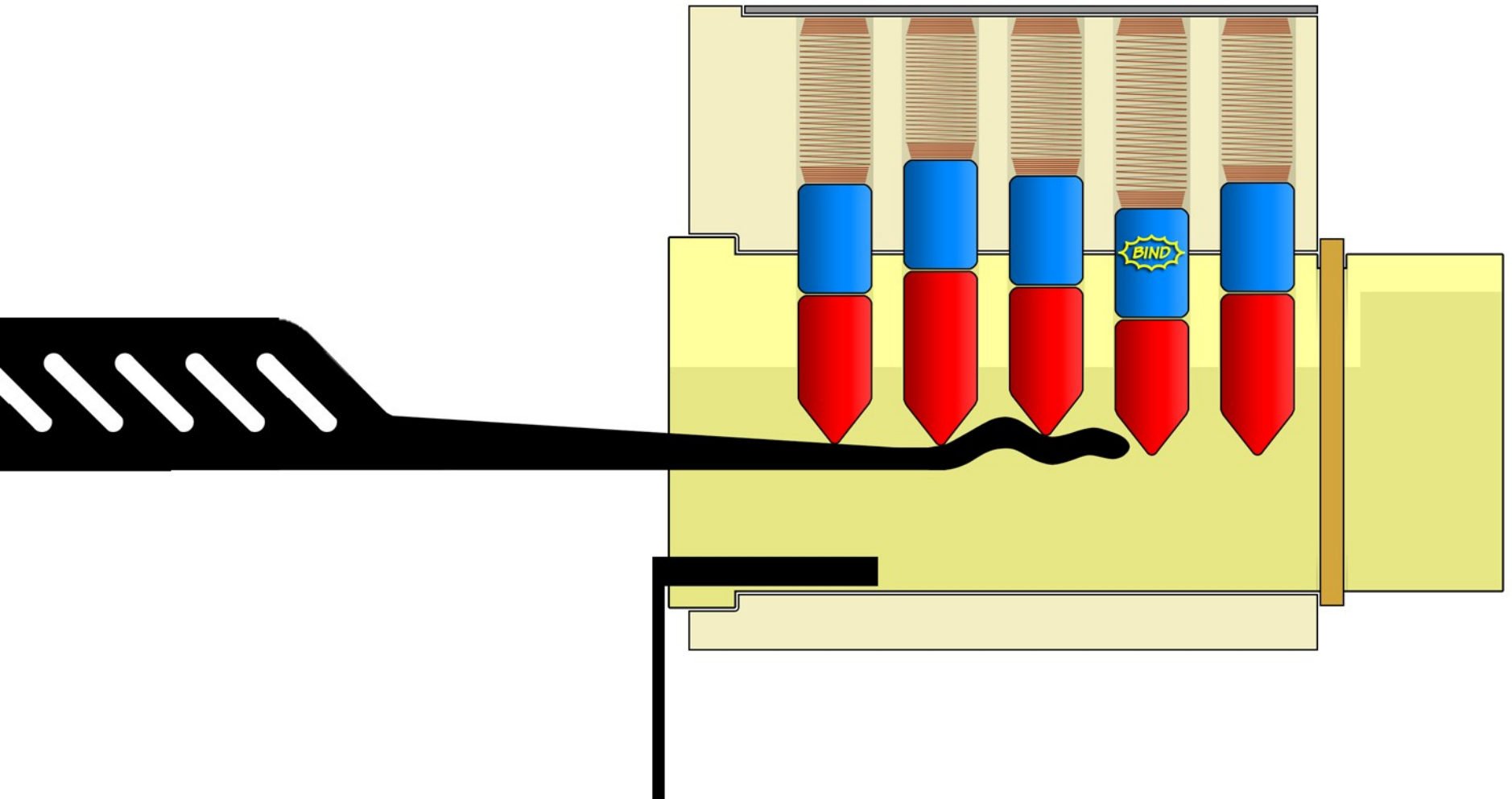




# Lifting Picking



# Raking

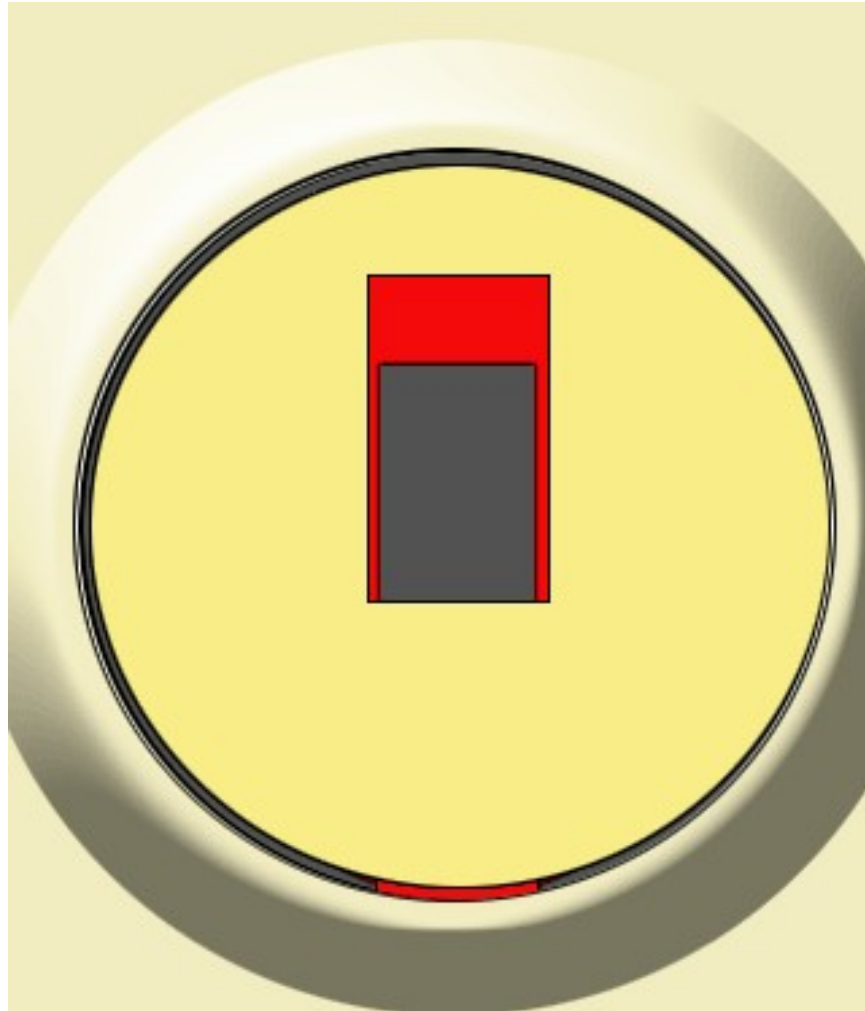




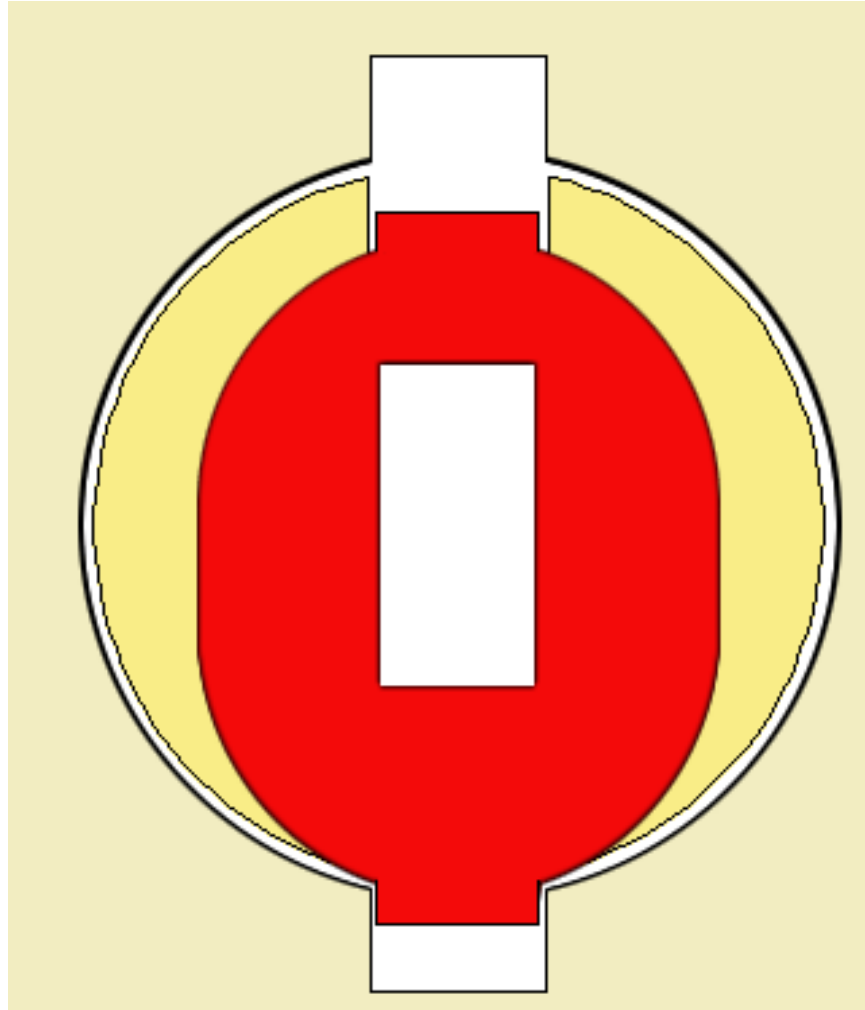
# Wafer Locks



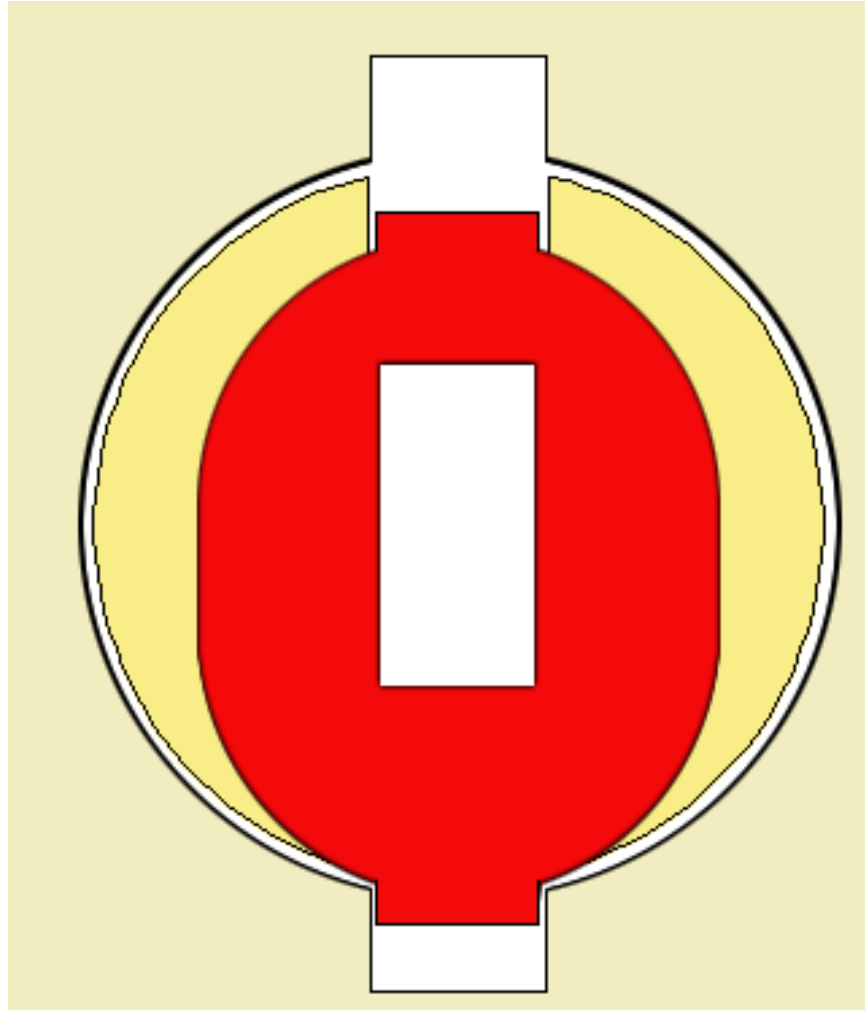
# Wafer Locks



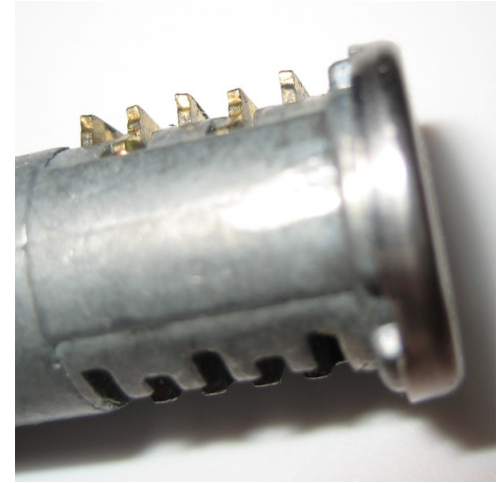
# Wafer Locks



# Wafer Locks



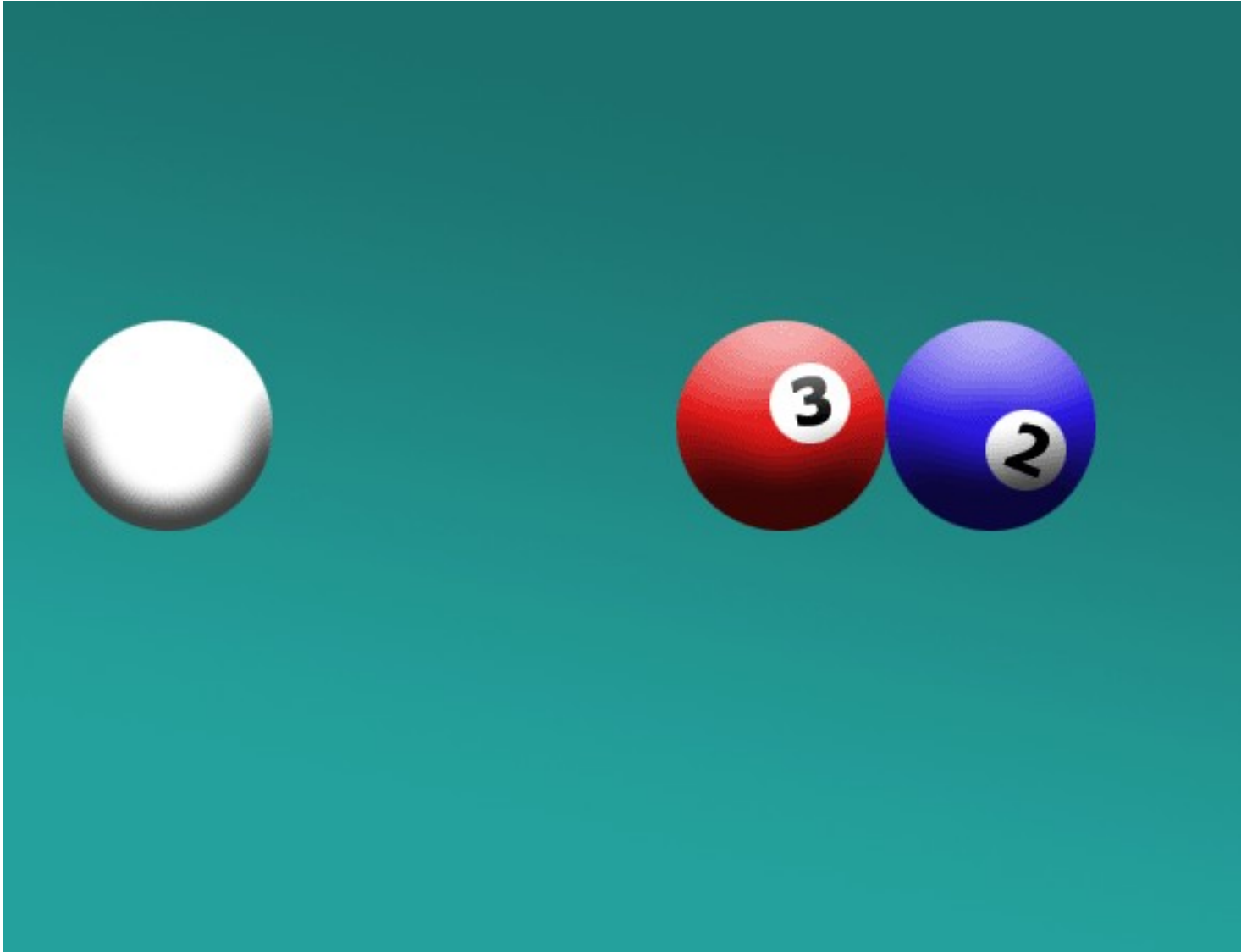
# Raking & Jiggling



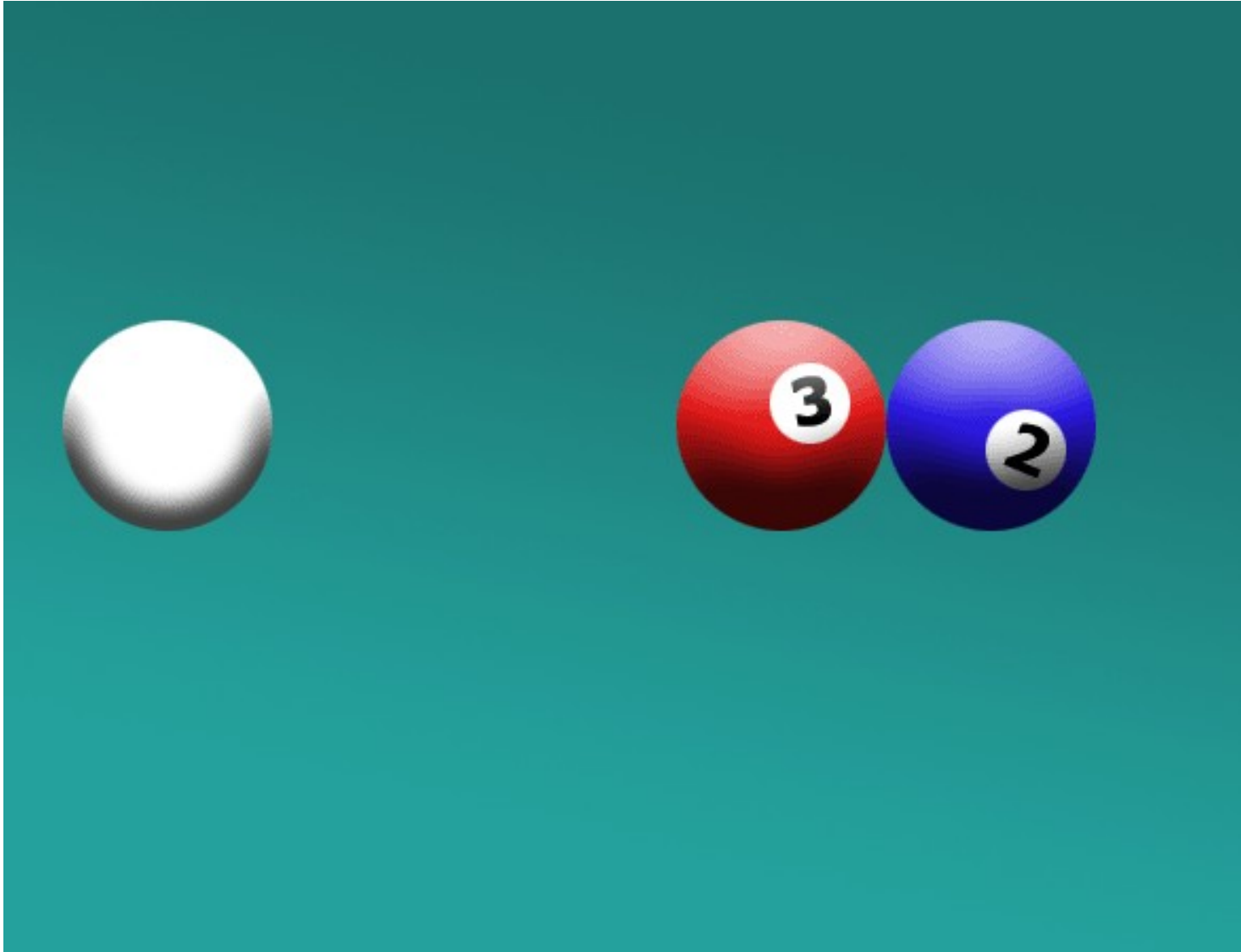
# Shimming



# Bumping

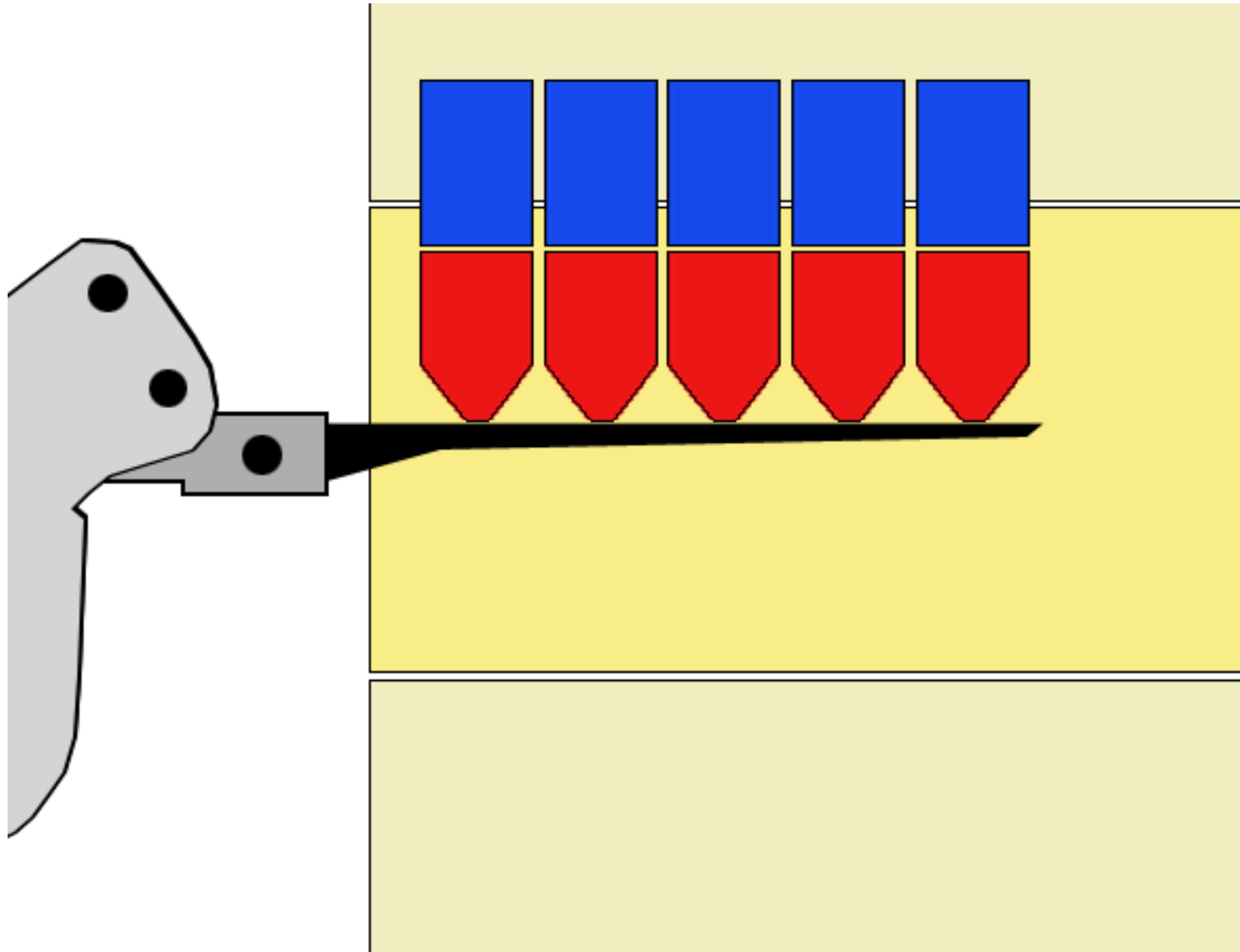


# Bumping



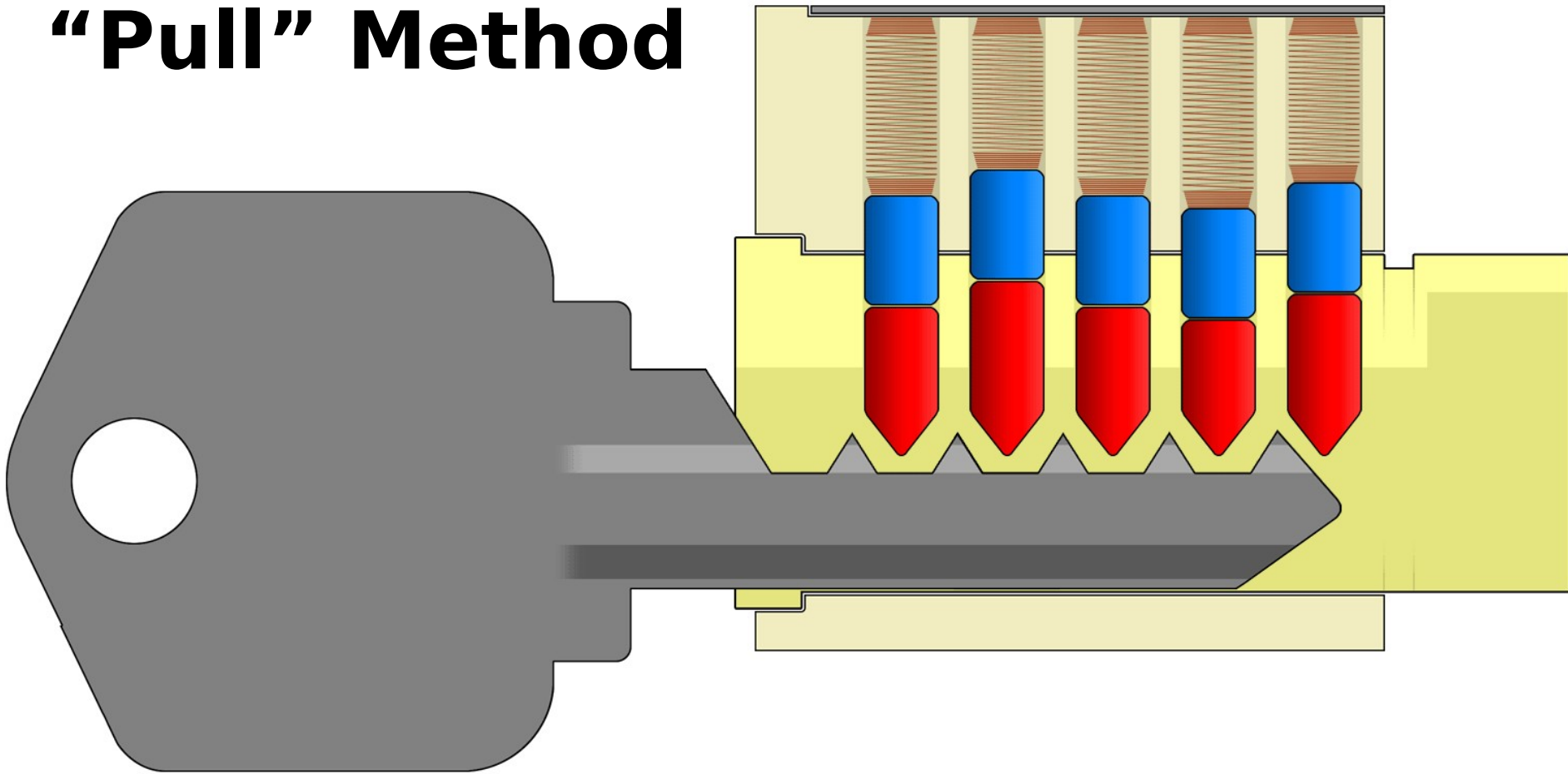


# Pick Guns



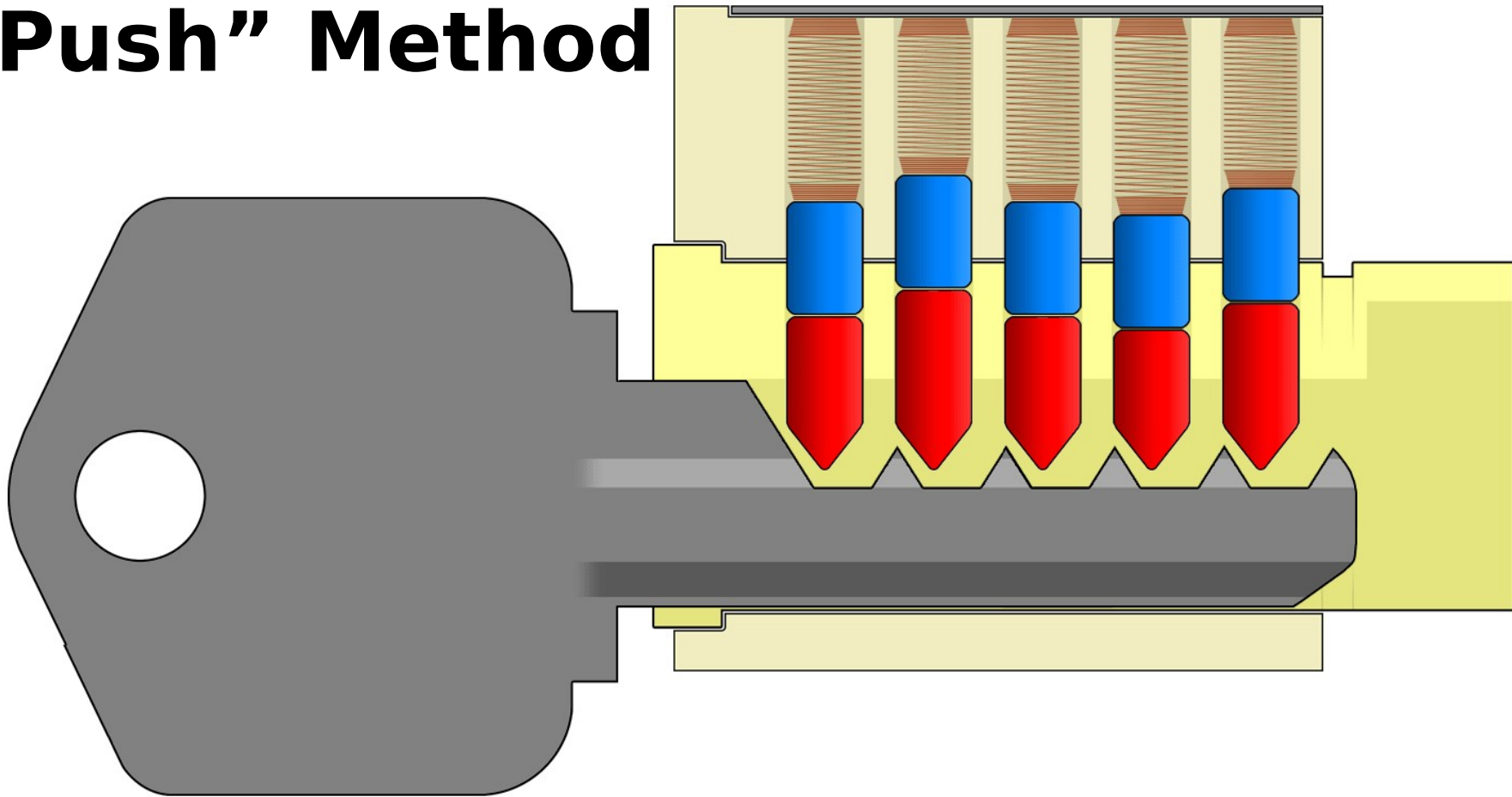
# Bump Key Attack

## “Pull” Method



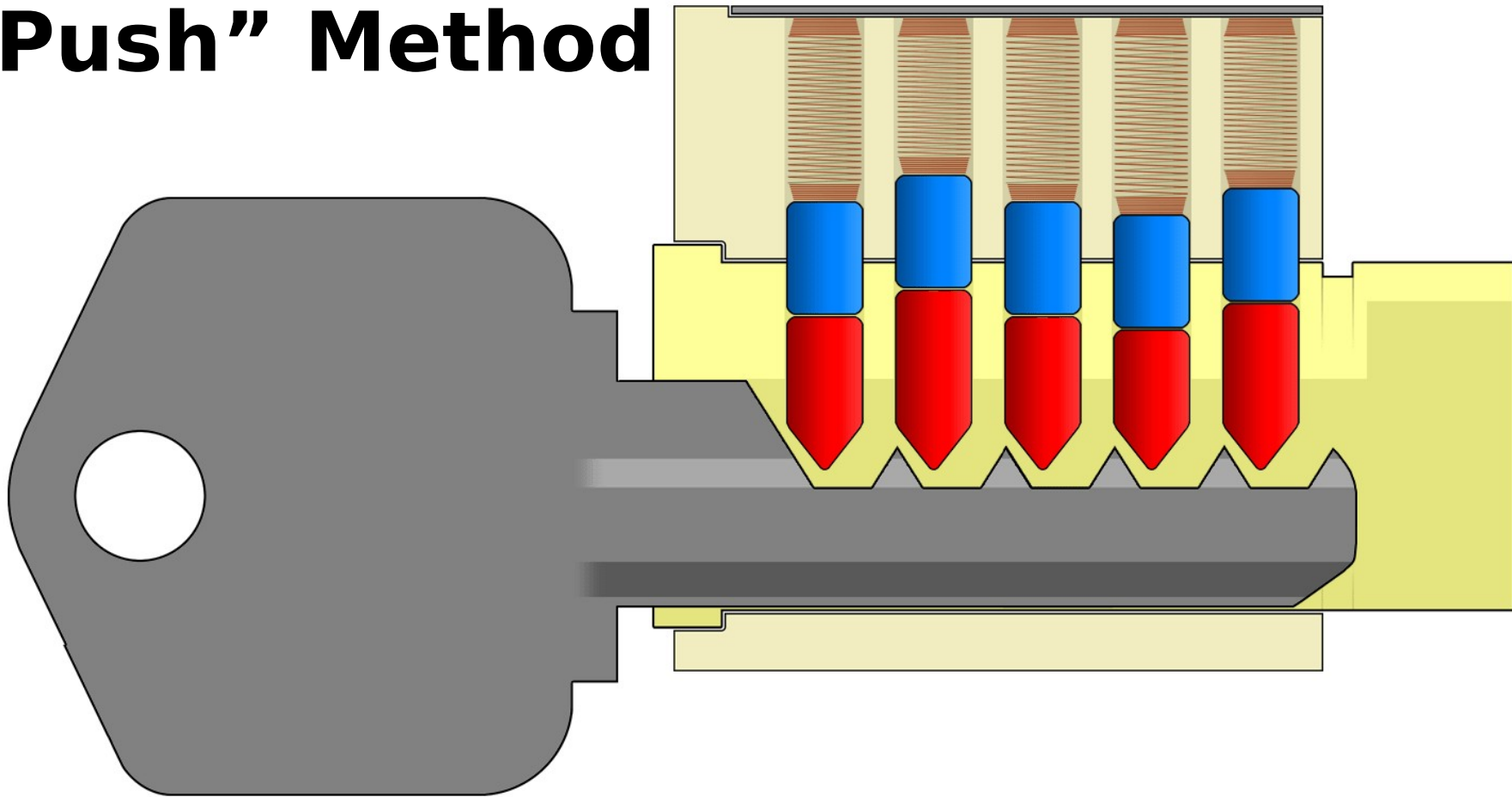
# Bump Key Attack

## “Push” Method

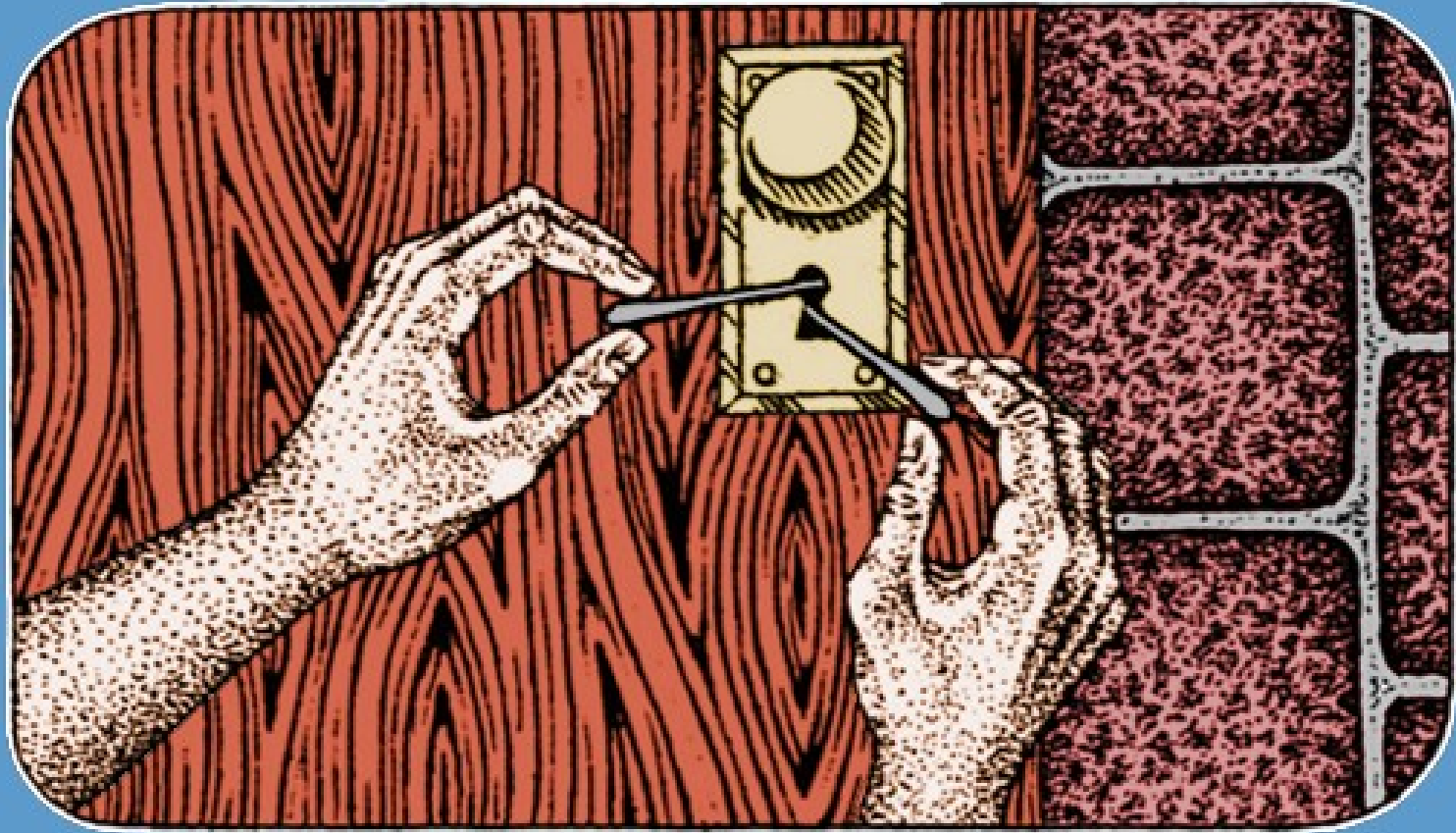


# Bump Key Attack

## “Push” Method



# Where are you using these weak locks ?





# Outdoor “Rugged” Locks



# Outdoor “Rugged” Locks



# Outdoor “Rugged” Locks



# Outdoor “Rugged” Locks





# Outdoor “Rugged” Locks





# Outdoor “Rugged” Locks

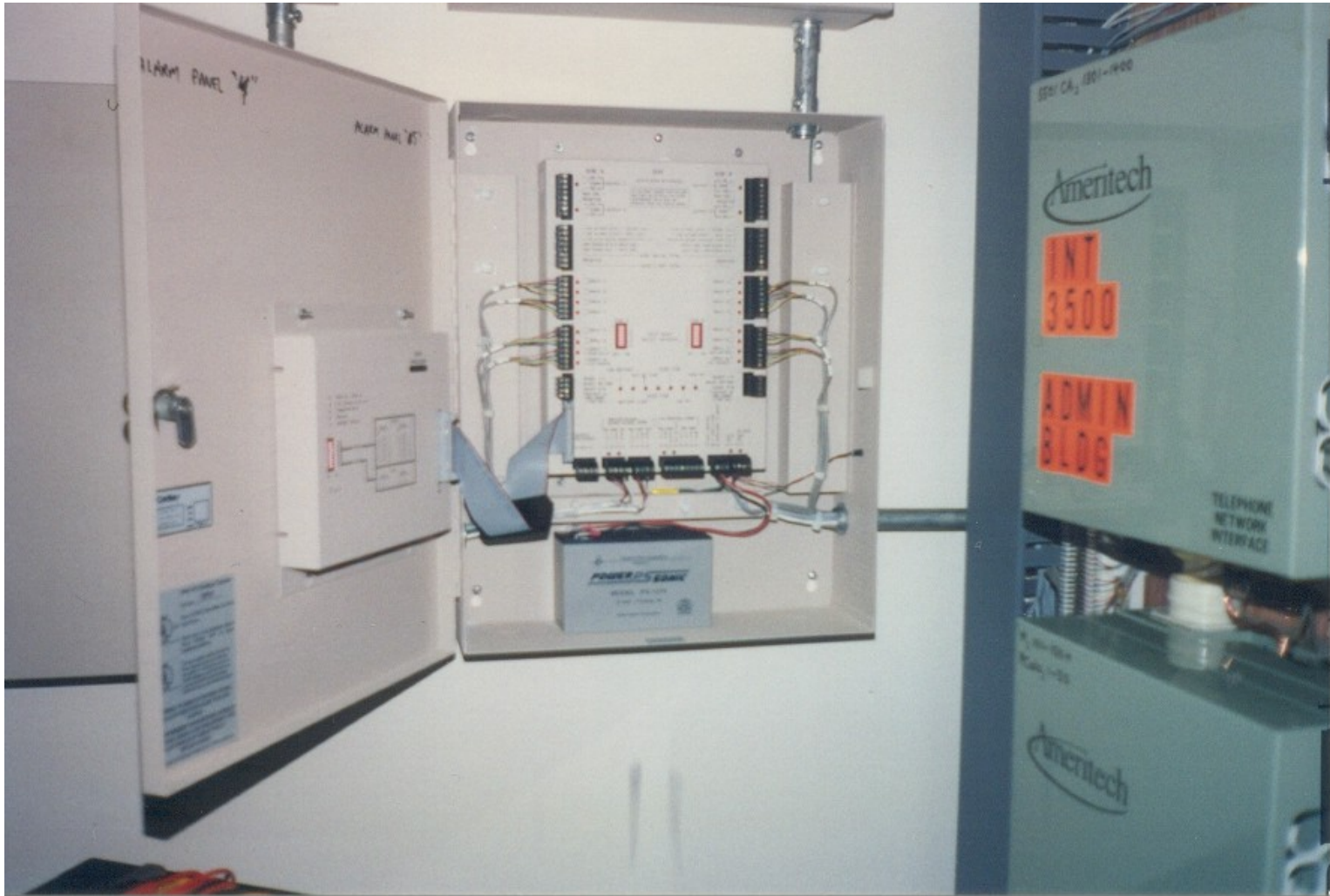




# Power Panels



# Sensitive Wiring





# Sensitive Wiring

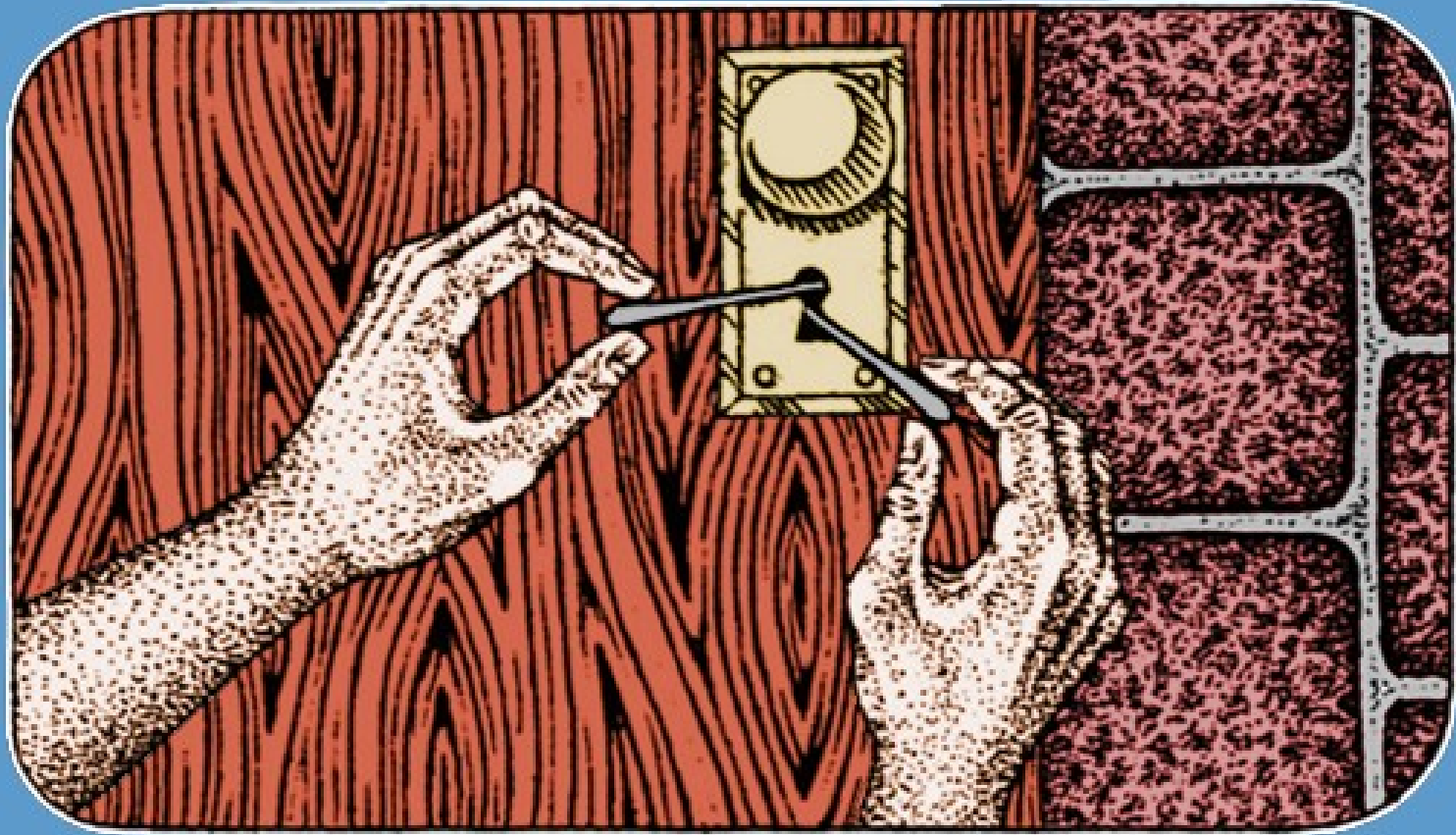




# Sensitive Wiring



# Why are most locks this bad?



# It's a Problem of Standards

- **American National Standards Institute**
- **Classification A156**
- **No Covert Security Ratings At All**



- **American Society for Testing Materials**
- **Classification F883**
- **Toughest Rating is only 15 minutes**



# Many Times, Picking is Instantaneous





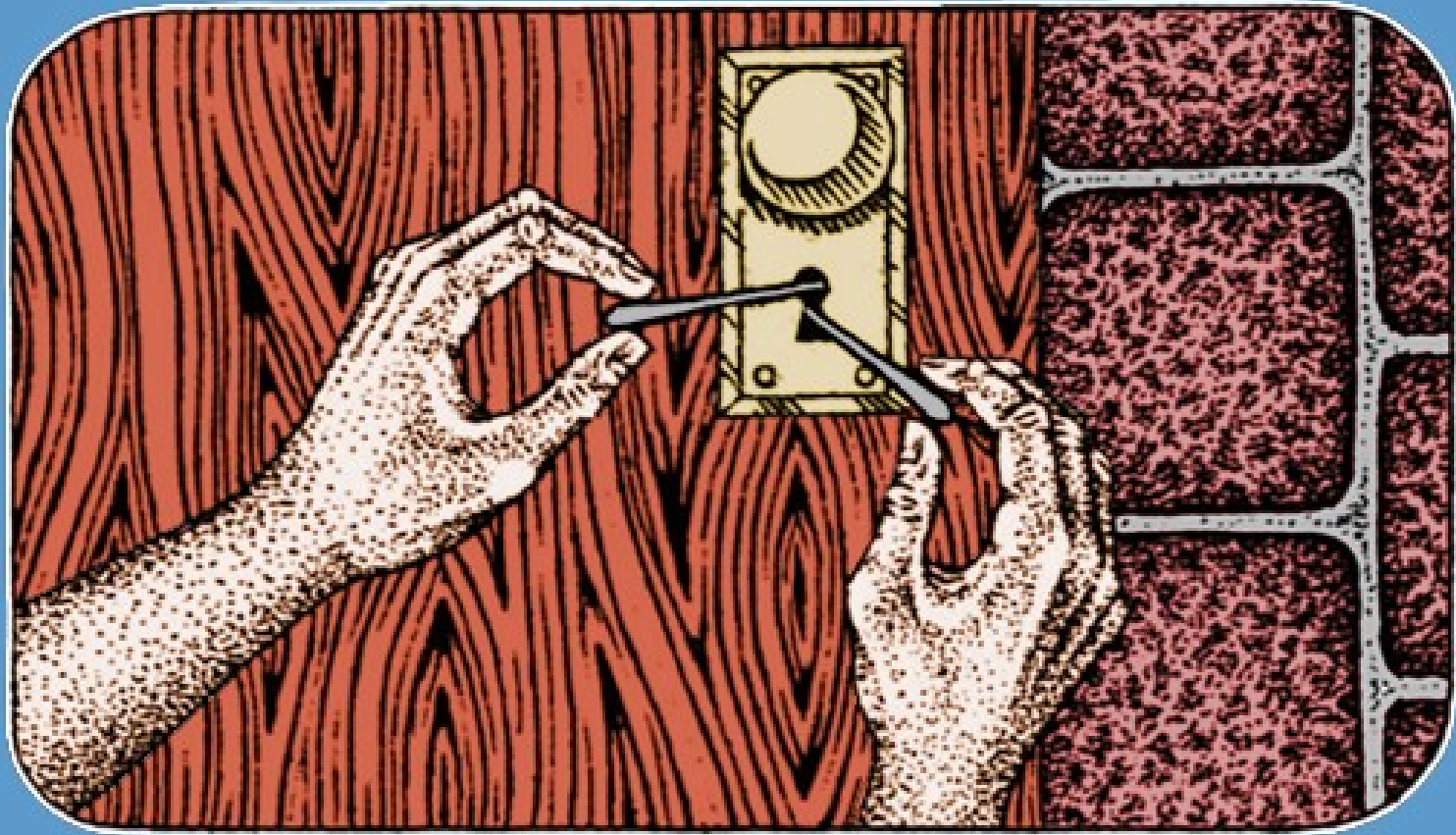
# You Need a Response Window





# One Step Up...

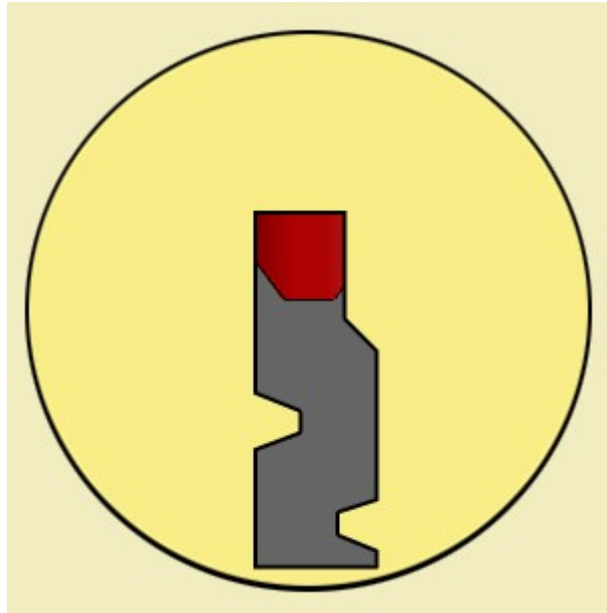
## “Pick Resistant” Locks



# Advanced Keyways

- **Simple...**

**straight and**



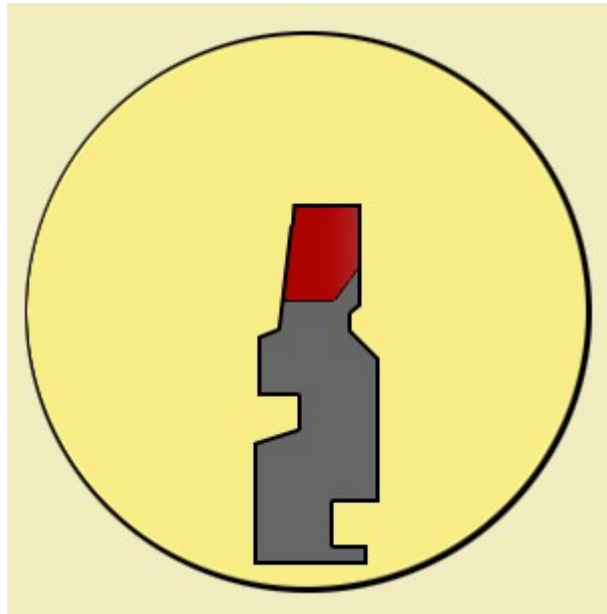
# Advanced Keyways

- **Simple...**

**straight and**

- **Medium...**

**straight but**



# Advanced Keyways

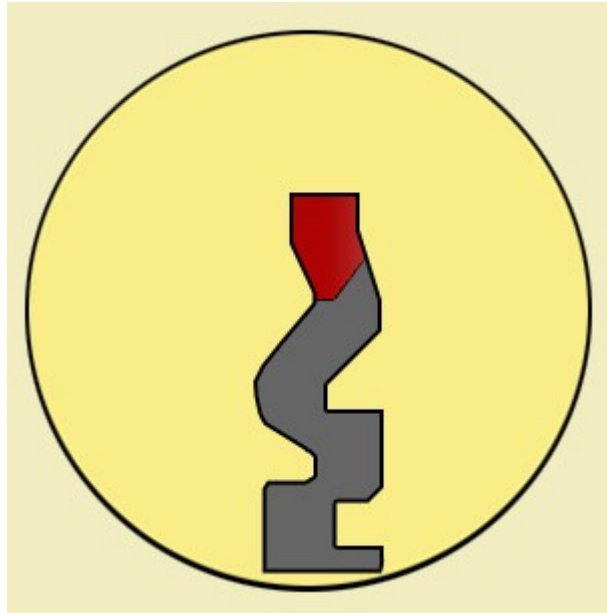
- **Simple...**

**straight and**

- **Medium...**

**straight but**

- **Complex...**



# Advanced Keyways

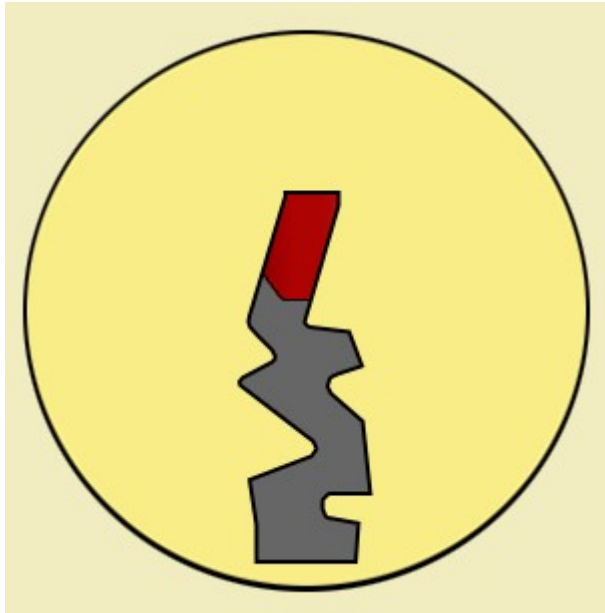
- **Simple...**

**straight and**

- **Medium...**

**straight but**

- **Complex...**





# Advanced Keyways

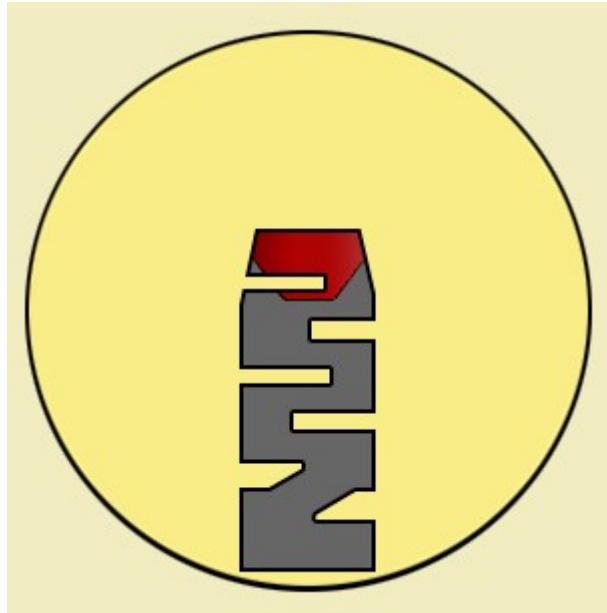
- **Simple...**

**straight and**

- **Medium...**

**straight but**

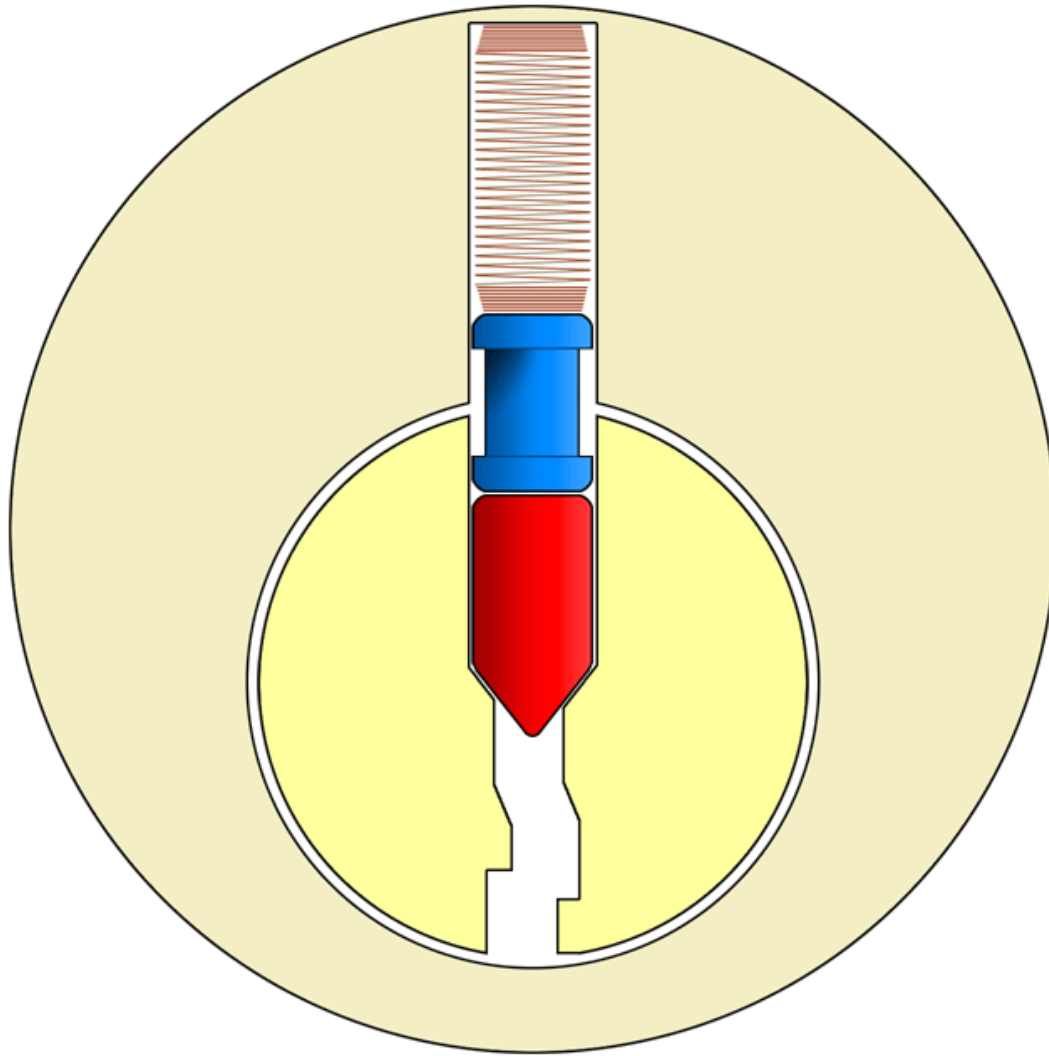
- **Complex...**



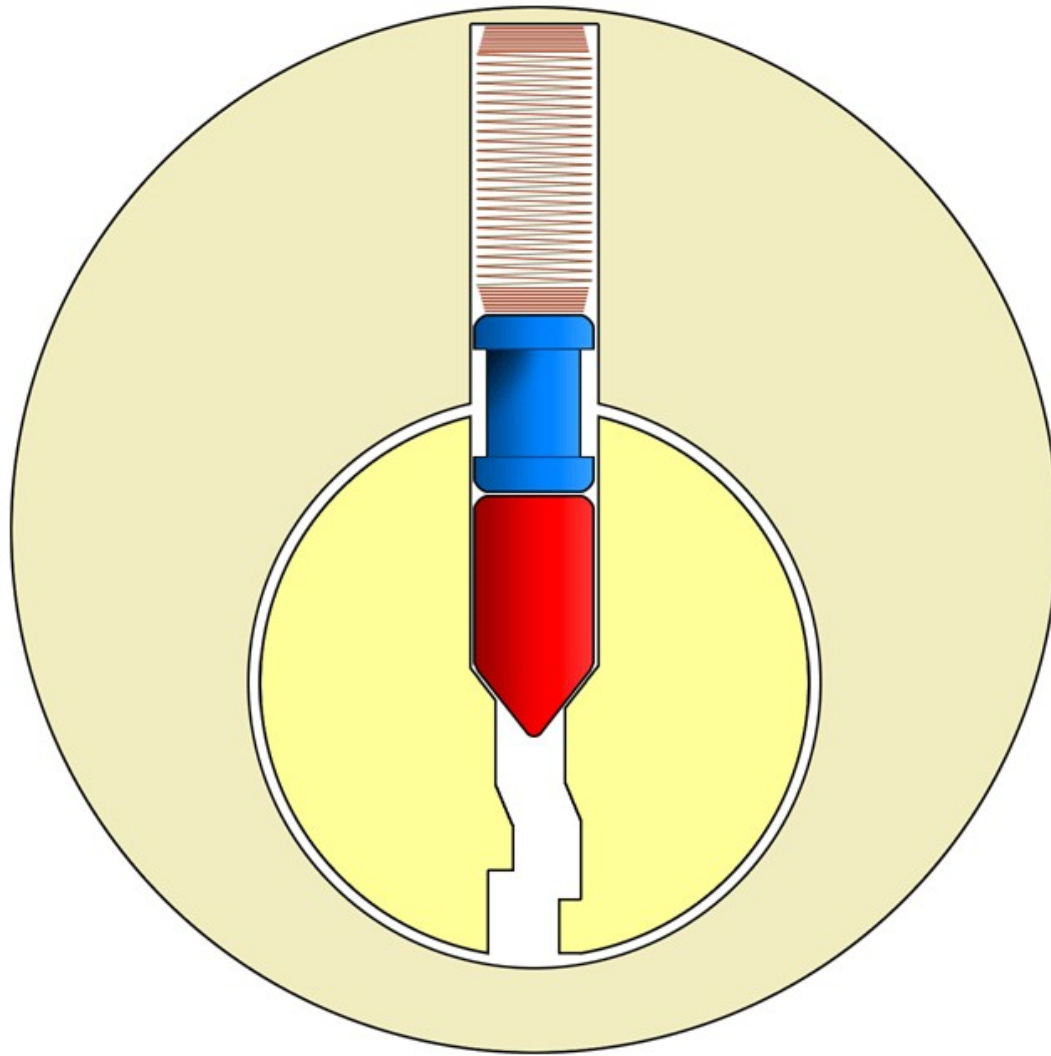
# Un-Shimmable Padlocks



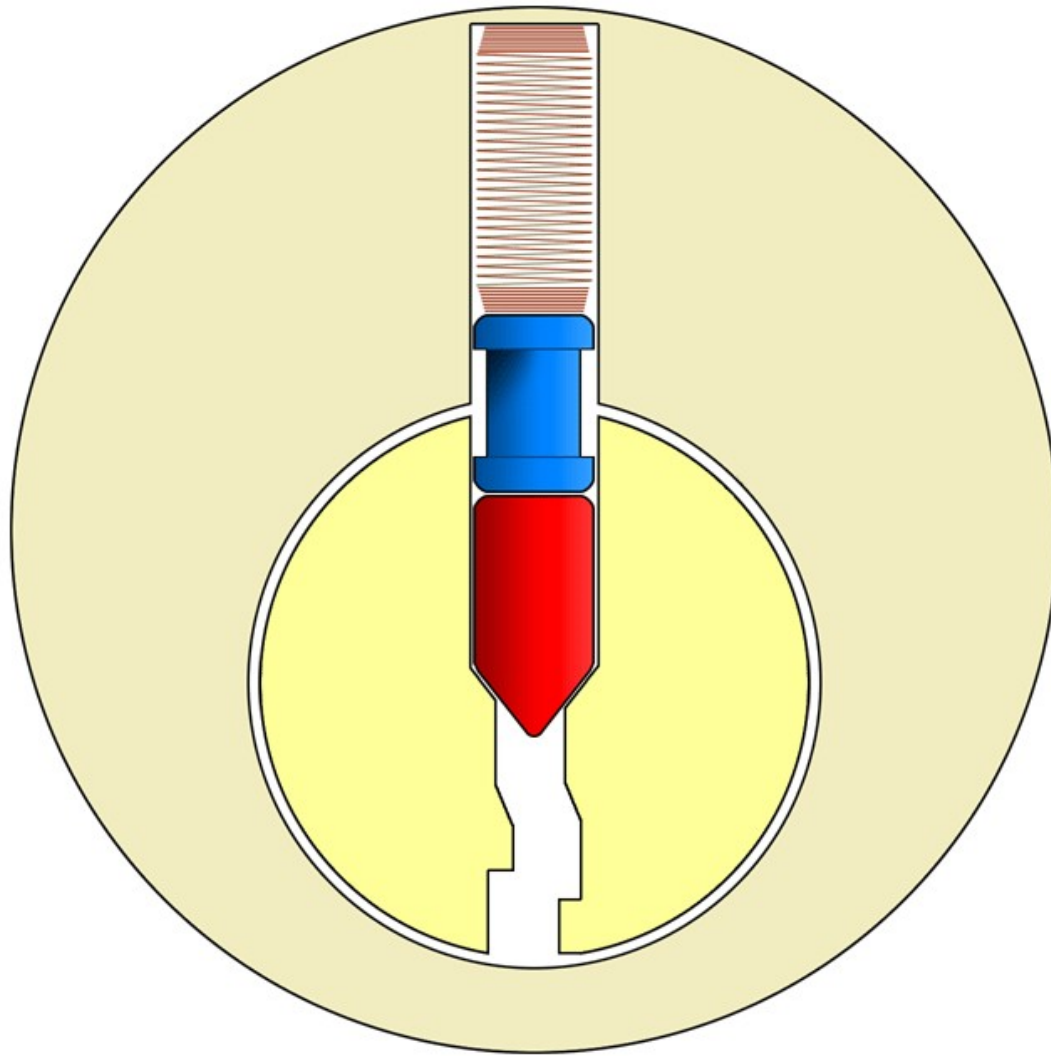
# Pick Resistant Pins



# Pick Resistant Pins

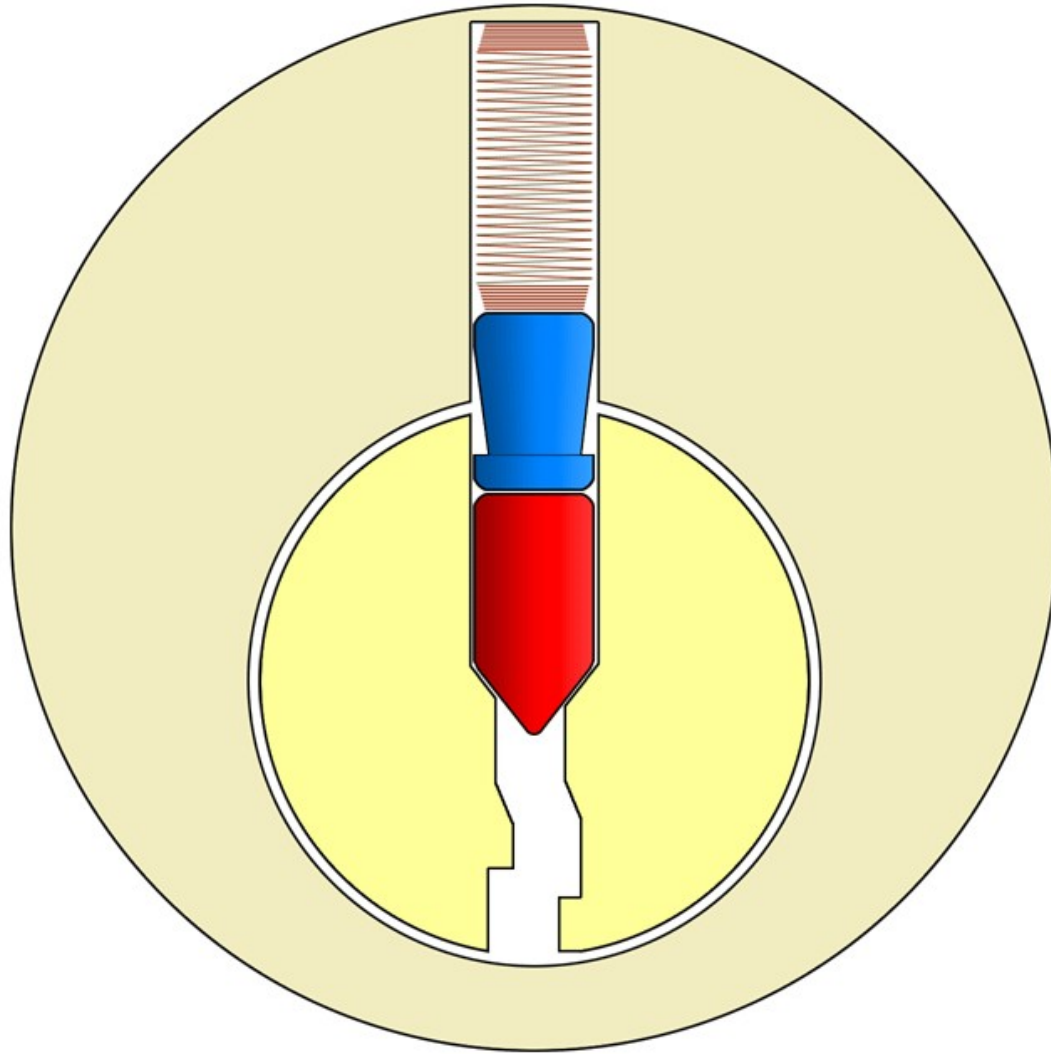


# Pick Resistant Pins

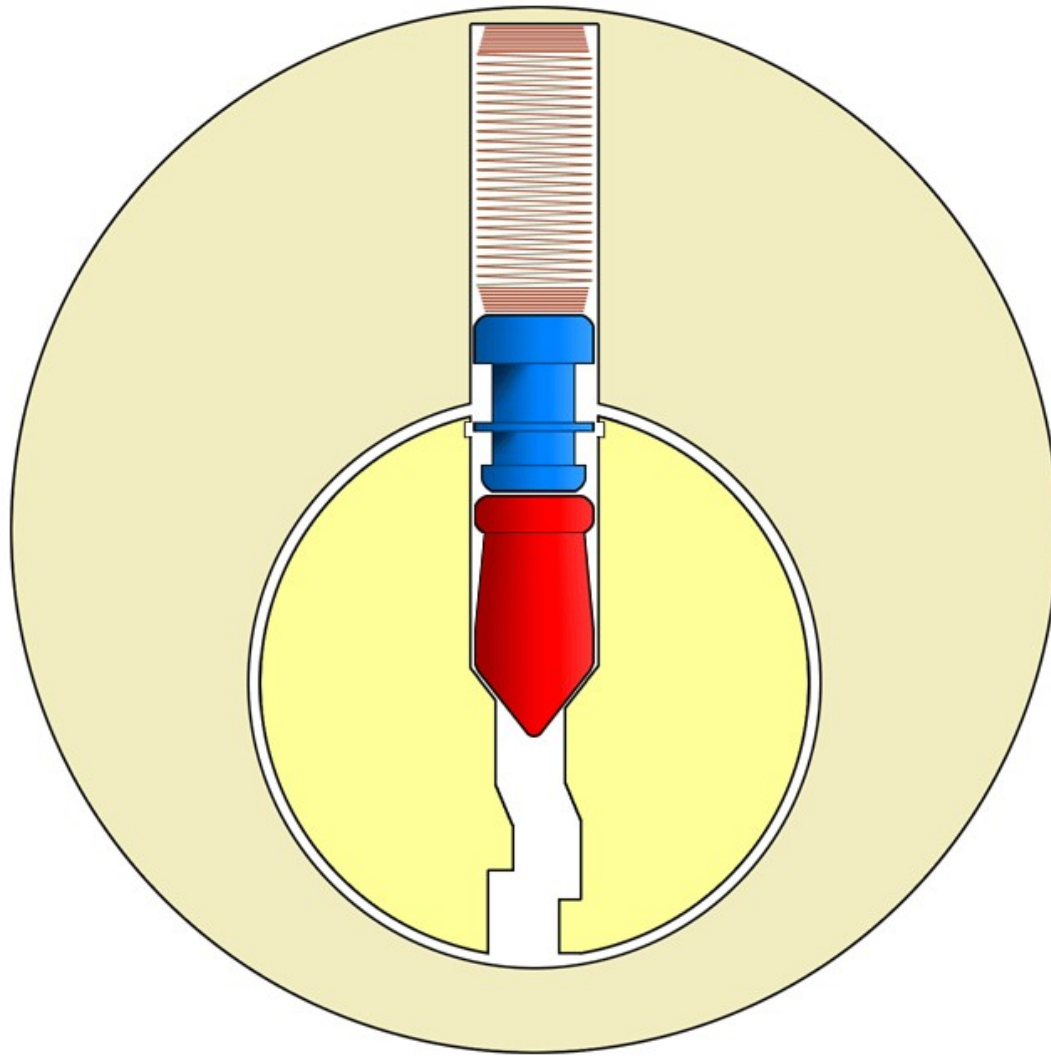




# Pick Resistant Pins

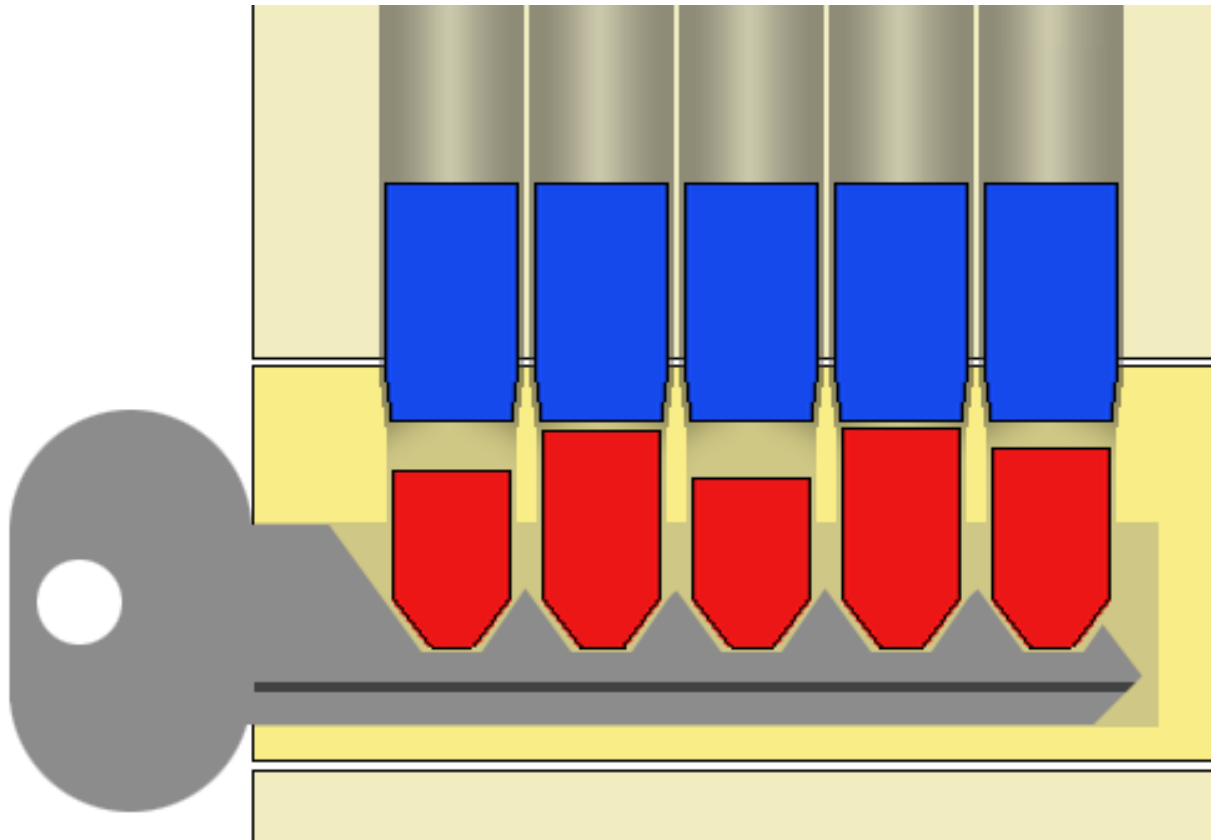


# Pick Resistant Pins



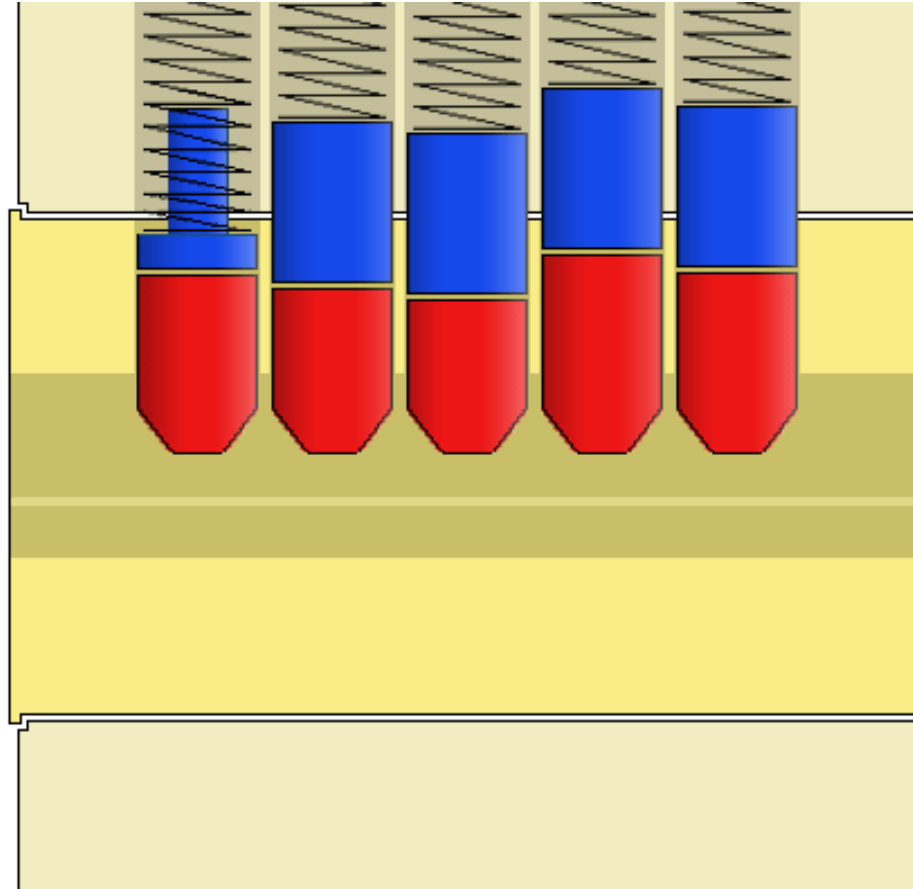
# Bump-Resistant Pins

## Top Gapping



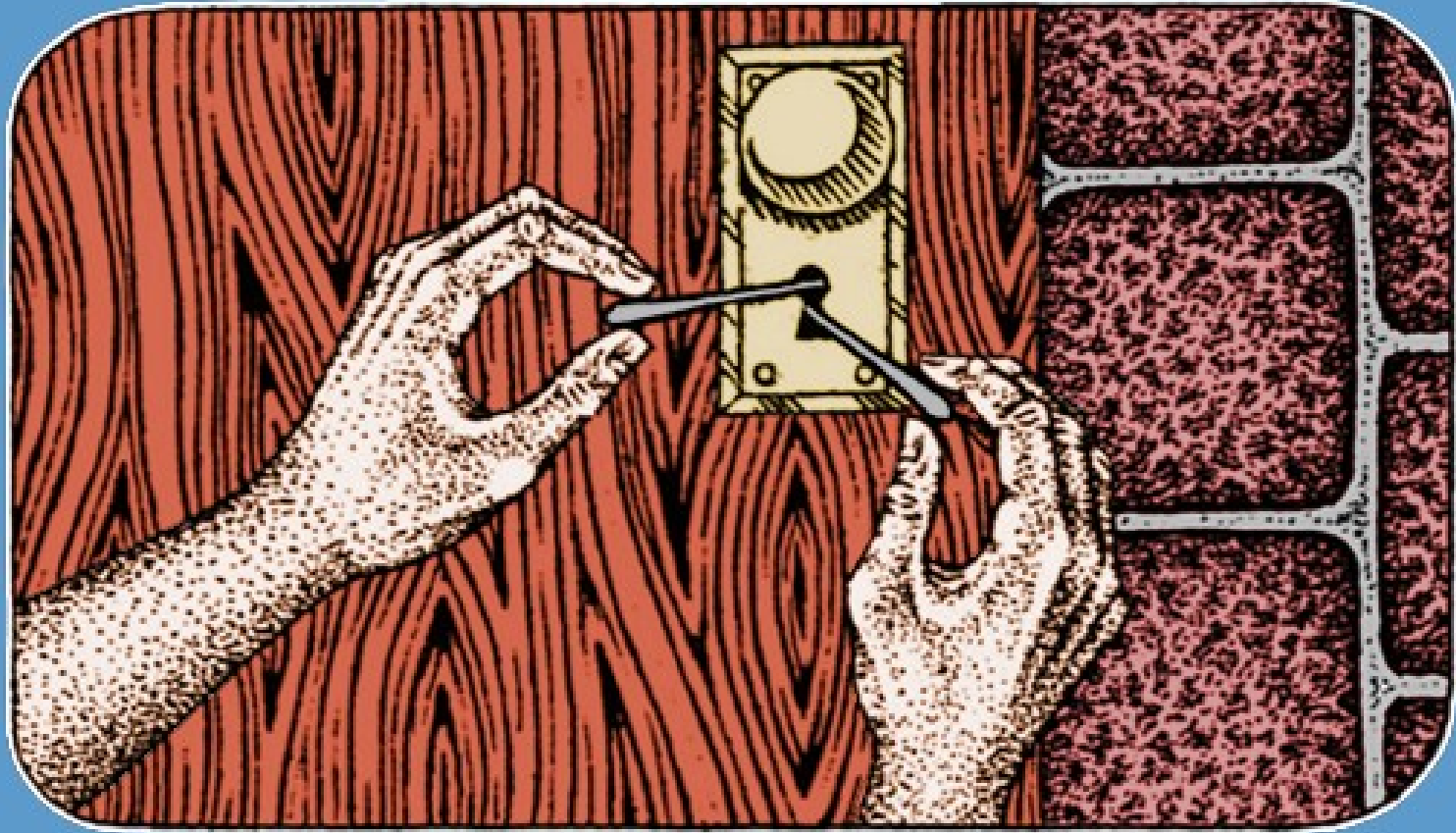
# Bump-Resistant Pins

## Anti-Bump Driver Pin



# The Next Step Up...

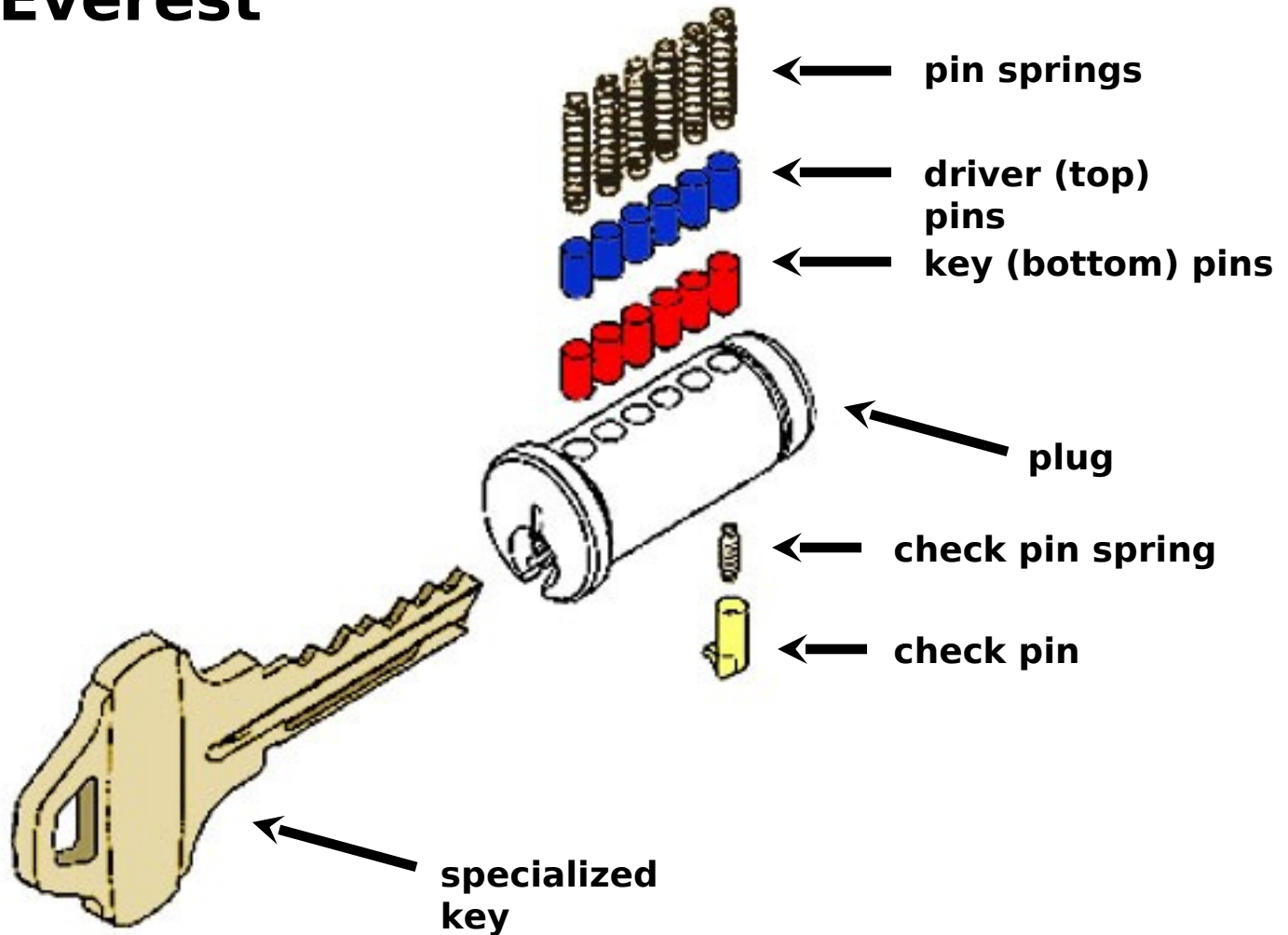
## “High Security” Locks





# Side Pin

## Schlage Everest



# Side Pin

## Schlage Everest



photos courtesy of Matt Blaze

# Side Pin

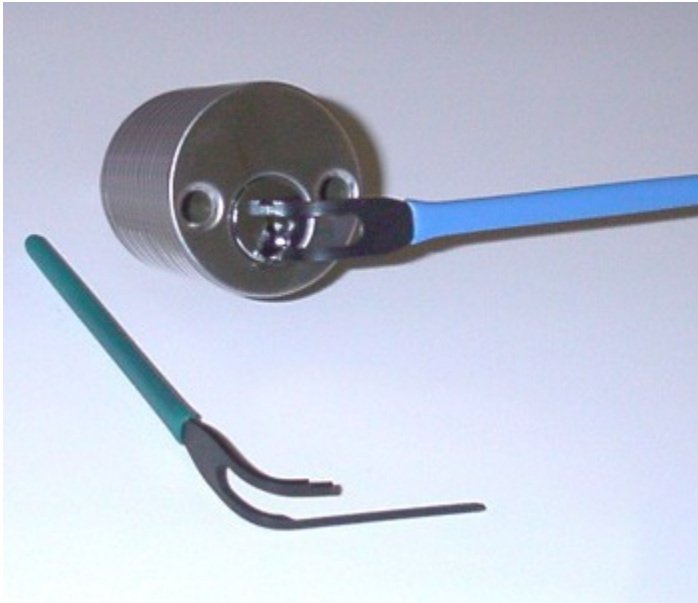
## Schlage Everest



photos courtesy of Matt Blaze

# Side Pin

## Schlage Everest



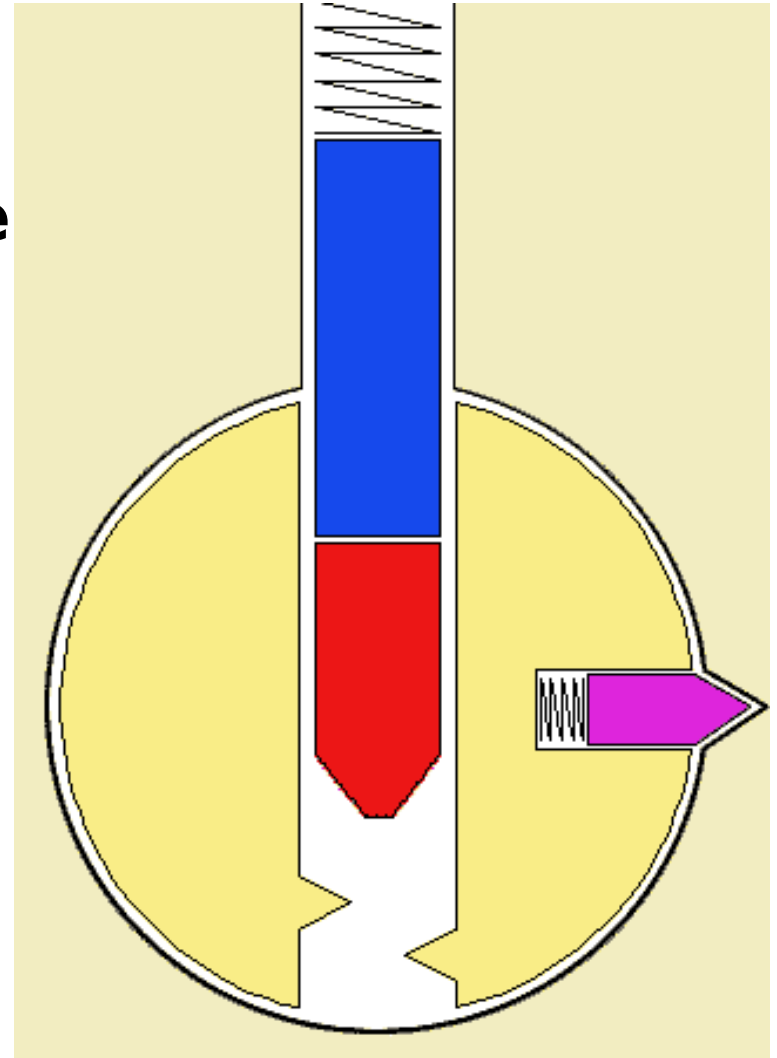
specialized “finger tensioner”



modified Everest key

# Side Bars

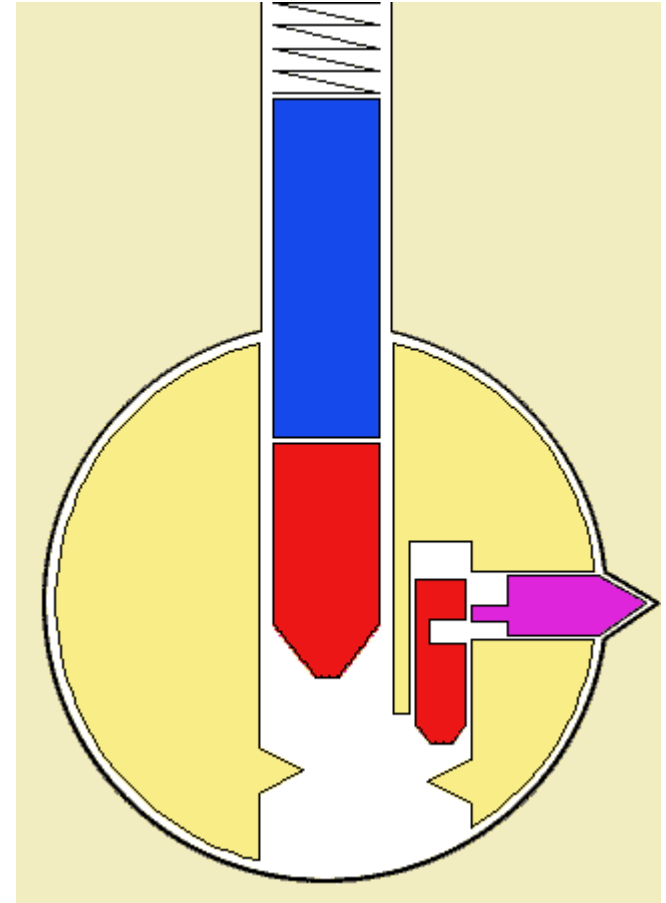
- **Similar to side pins**
- **Restrict plug moveme**
- **Harder to pick than pin stacks**





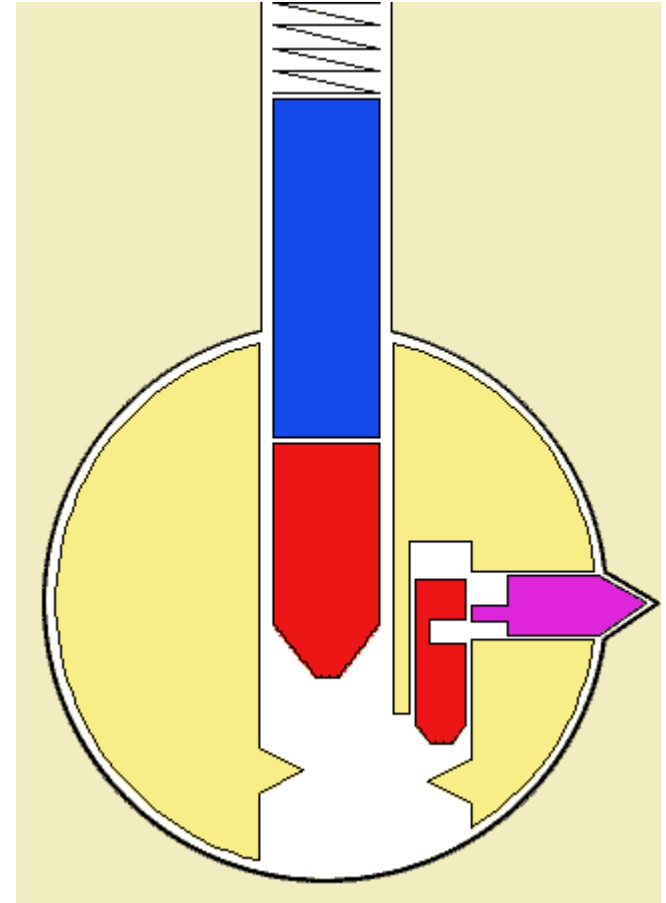
# Side Bars

## Finger Pins



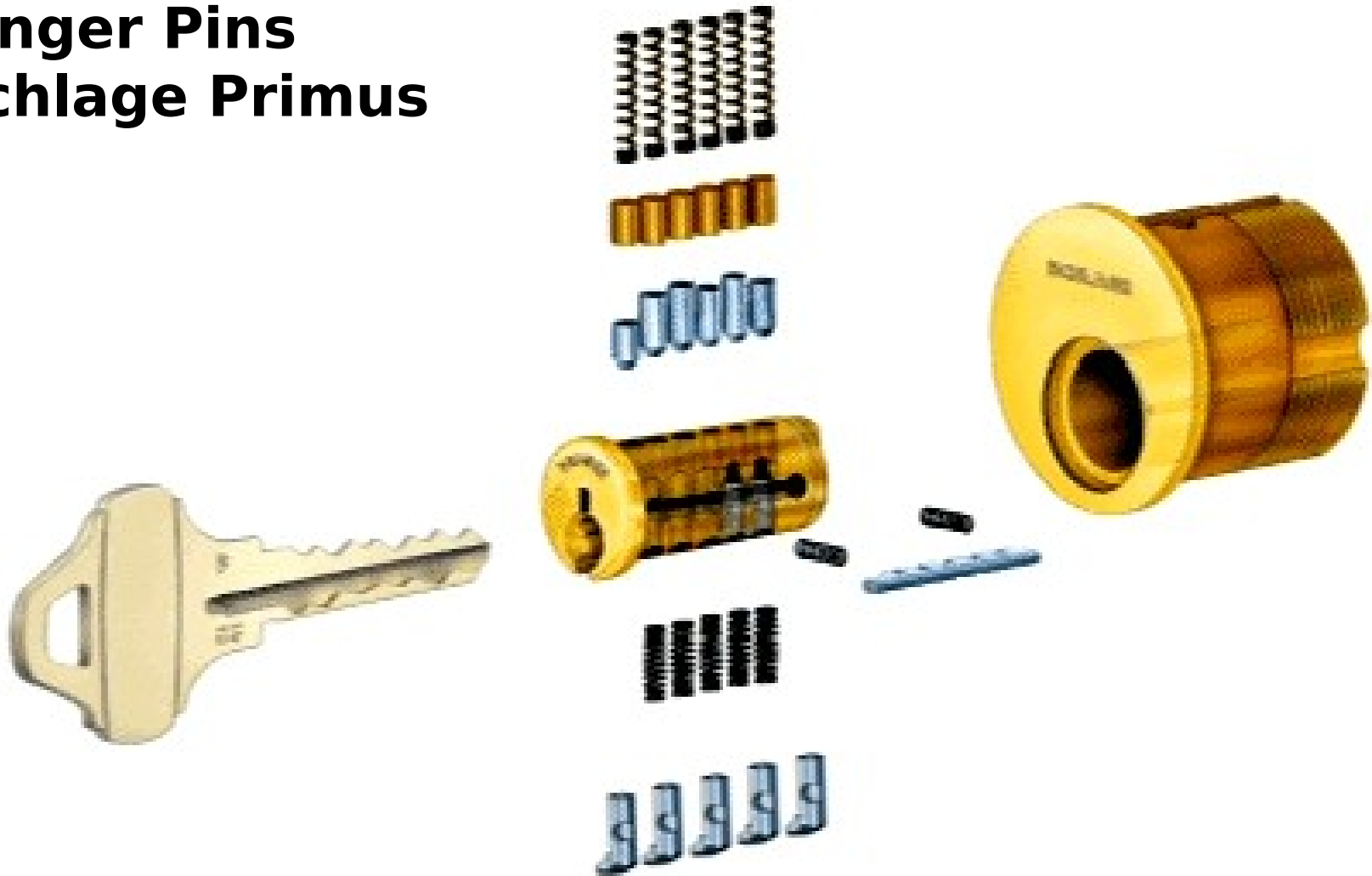
# Side Bars

## Finger Pins



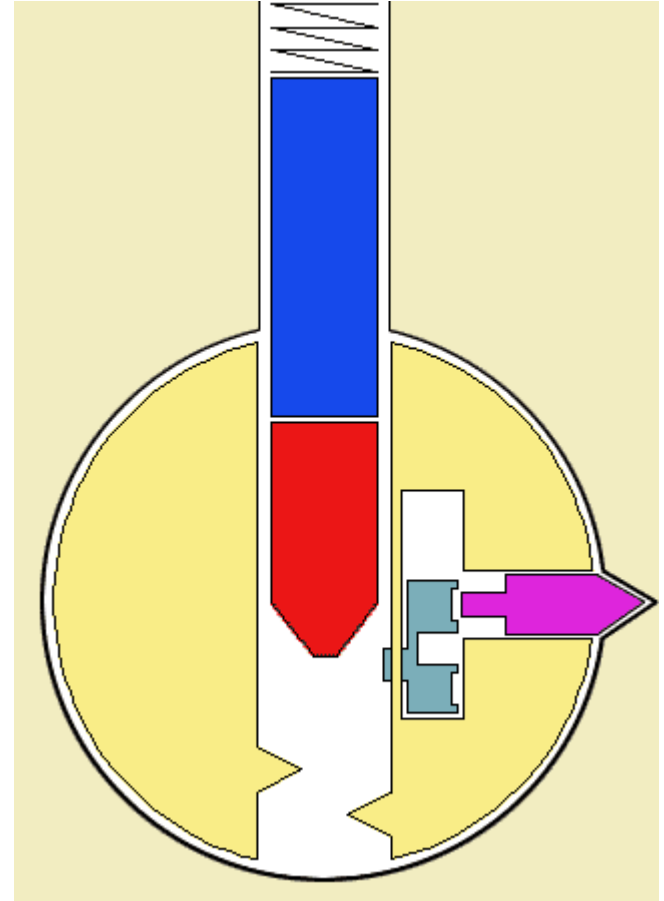
# Side Bars

**Finger Pins**  
**Schlage Primus**



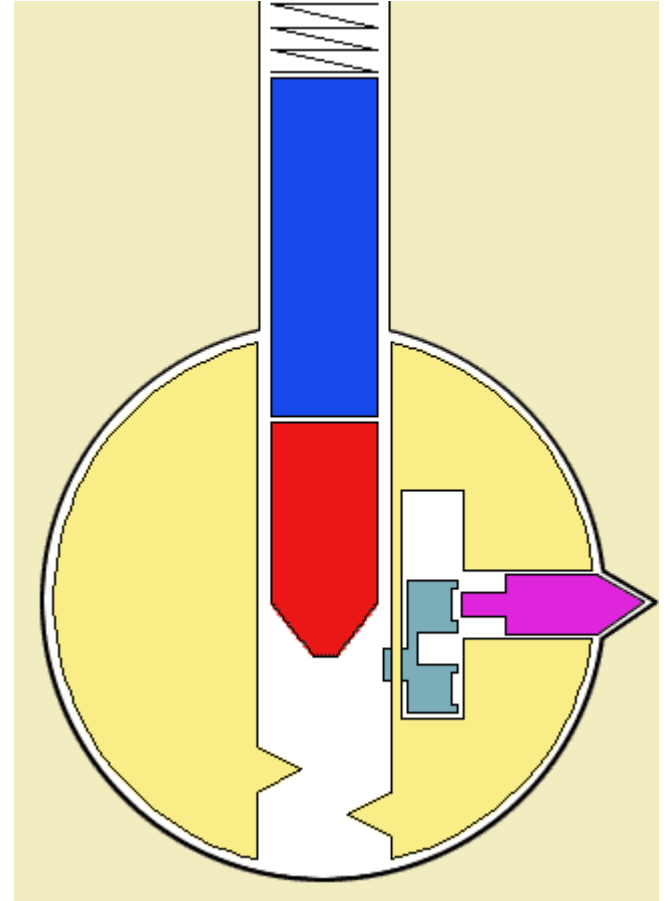
# Side Bars

## Sliders



# Side Bars

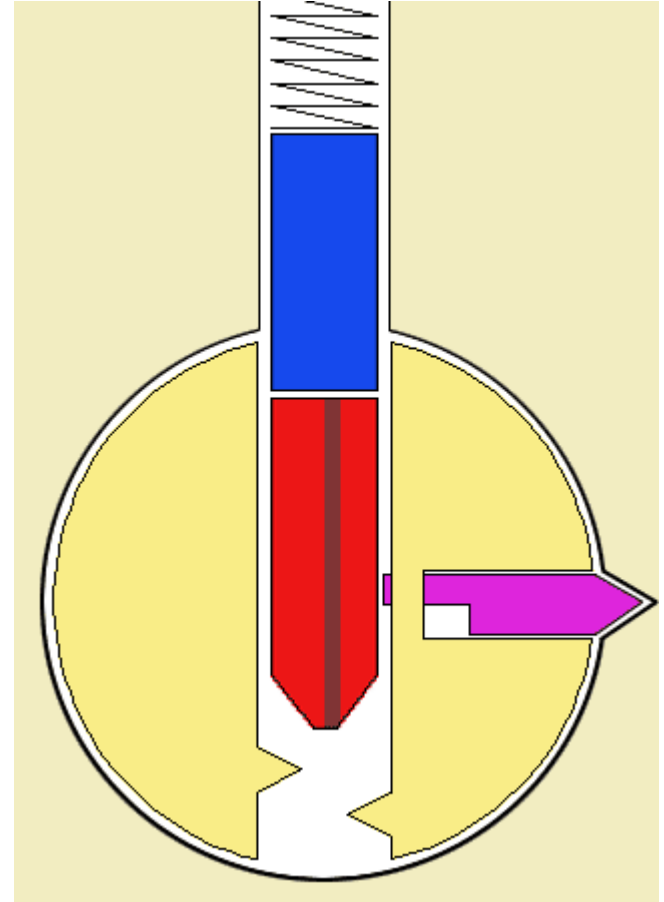
## Sliders





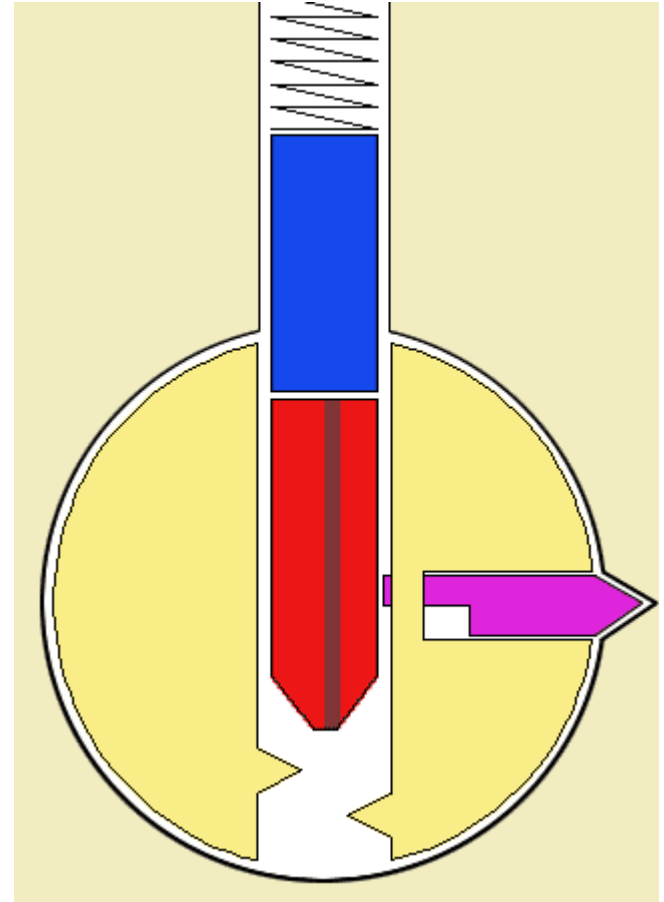
# Side Bars

## Rotating Pir



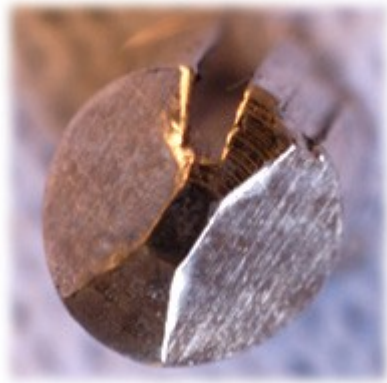
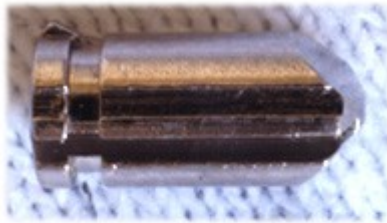
# Side Bars

## Rotating Pir



# Rotating Pins

## Medeco Locks



Medeco plug exposed, key pins rotating to align sidebar cuts



Top View



Side View

# Rotating Pins

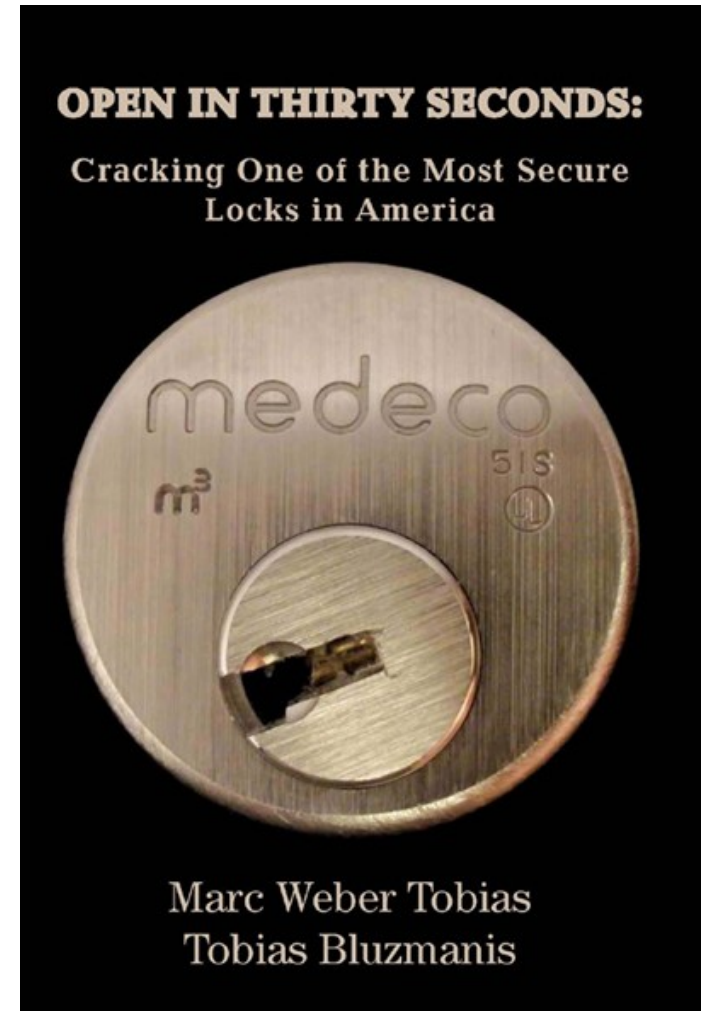
## Medeco locks

### certainly not “unpickable”

- Can be picked
- Can be bumped
- Numerous weaknesses

- **“Open in 30 Seconds”**

- Marc Tobias
- Tobias Bluzmanis



# Rotating Disks

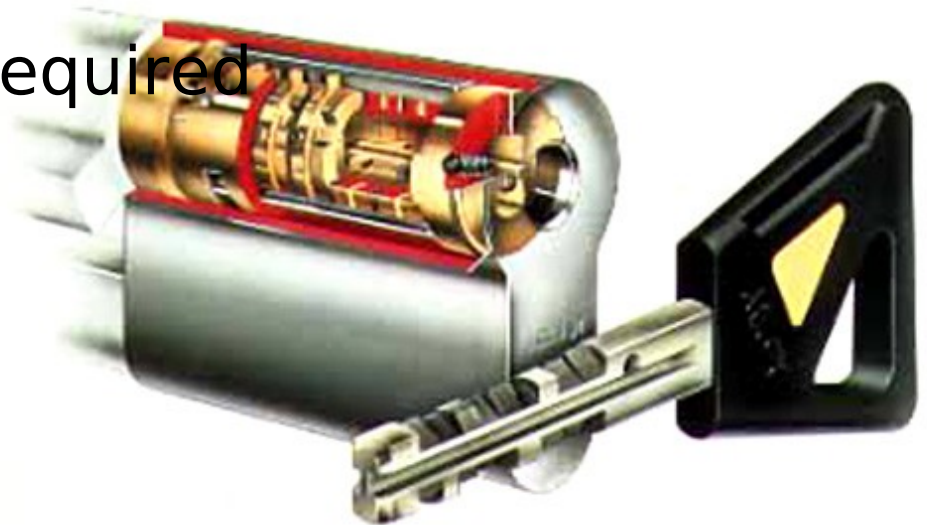
- **Sometimes Very Good**

## **Security**

- Mimics a safe lock

- **Difficult To Pick**

- Takes much time and great skill
- Specialized tools required





# Rotating Disks

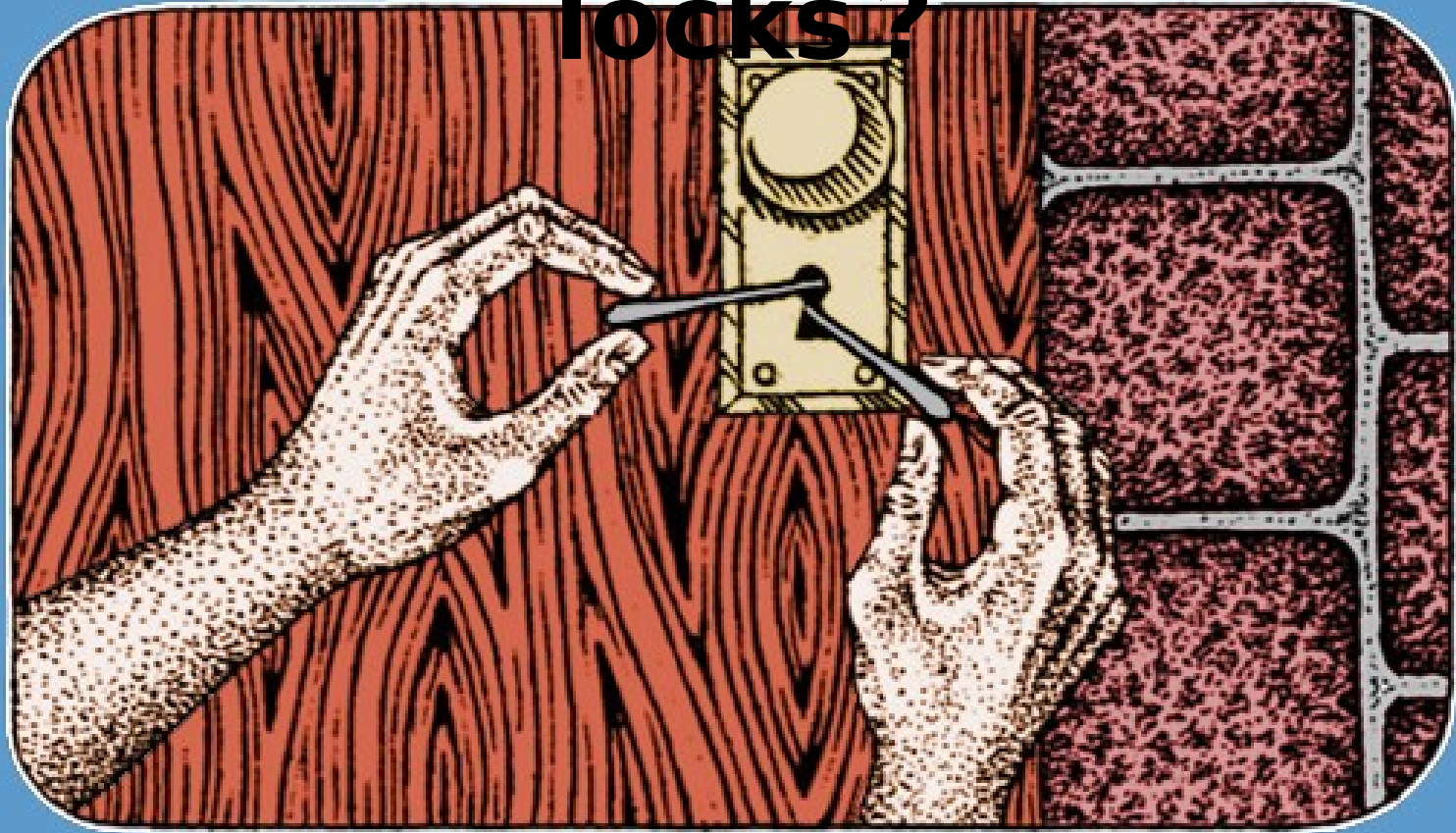
- **Sometimes Very Good Security**
  - Mimics a safe lock
- **Difficult To Pick**
  - Takes much time and great skill
  - Specialized tools required
- **Two-in-One Tool**
  - Manipulates disks individually
  - Decodes cut positions



Barry Wels picking a rotating disk lock with Mike Glasser

# The Highest Grade...

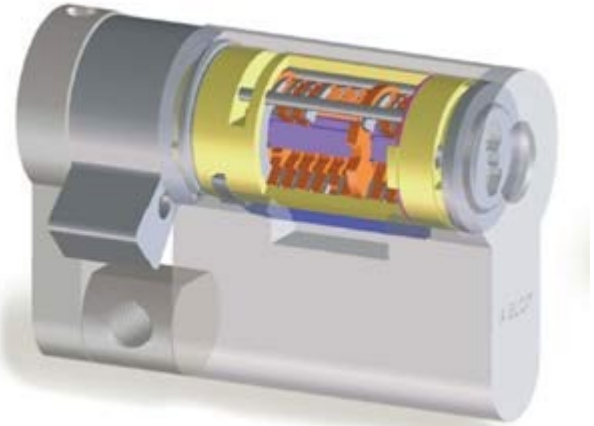
## Dare we say “unpickable” locks?



# Specialized Rotating Disks

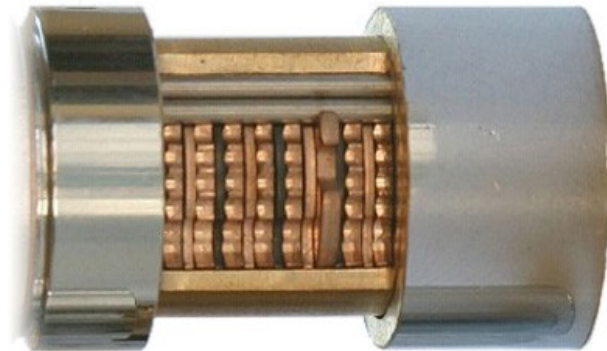
- **Abloy Protec**

- Not just rotating disks
- Disk blocking mechanism



- **“Unpickable?”**

- Closest I ever come to using that word
- Two-in-one tools cannot be used



# Certain Magnetic Locks

- **Miwa**

- Japanese company
- Array of magnetic pins
- Simple North / South



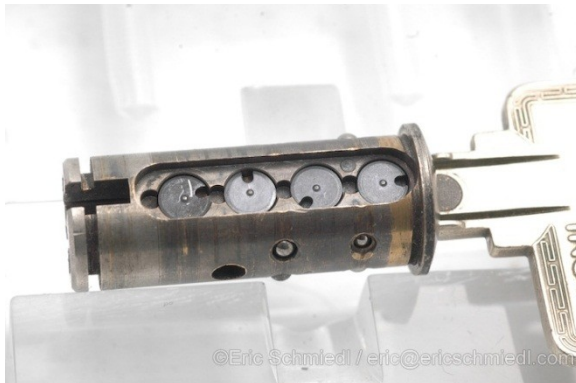
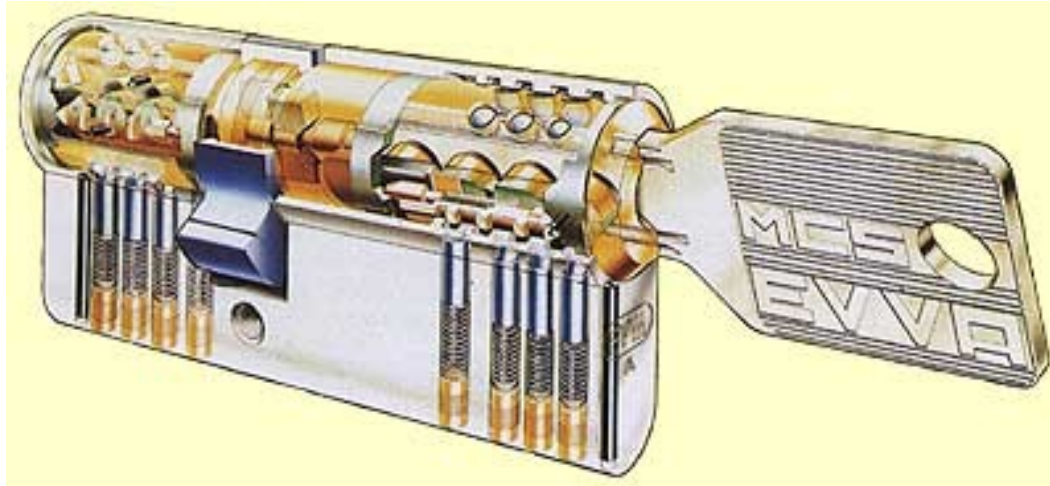
- **Evva MCS**

- Austrian company
- Axial-rotated magnets
- Interaction with sidebar



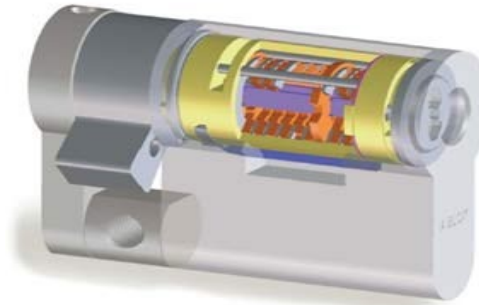
# Evva Magnetic Code System

- Possibly the most duplication-resistant lock





# No Known Attack or Bypass



 **ABLOY**

**Prote**  
**c**



**EVVA**

**MCS**



 **MUL-T-LOCK**

# What About Safes ?



photo courtesy of Don the  
Shadow

# What About Safes ?



# What About Safes ?



S&G 8400

# What About Safes ?



photo courtesy of Barry Wels

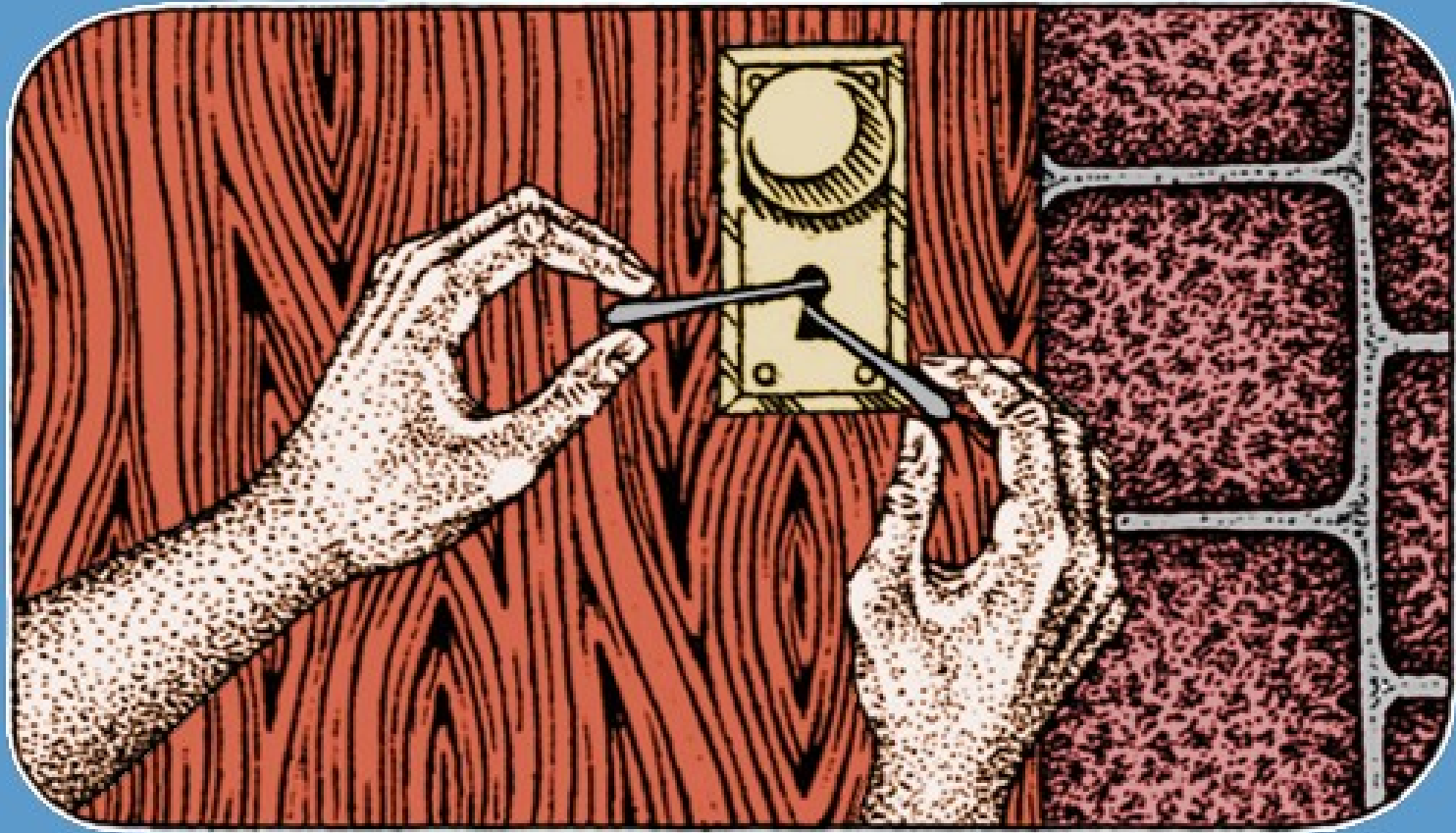


# What About Safes ?





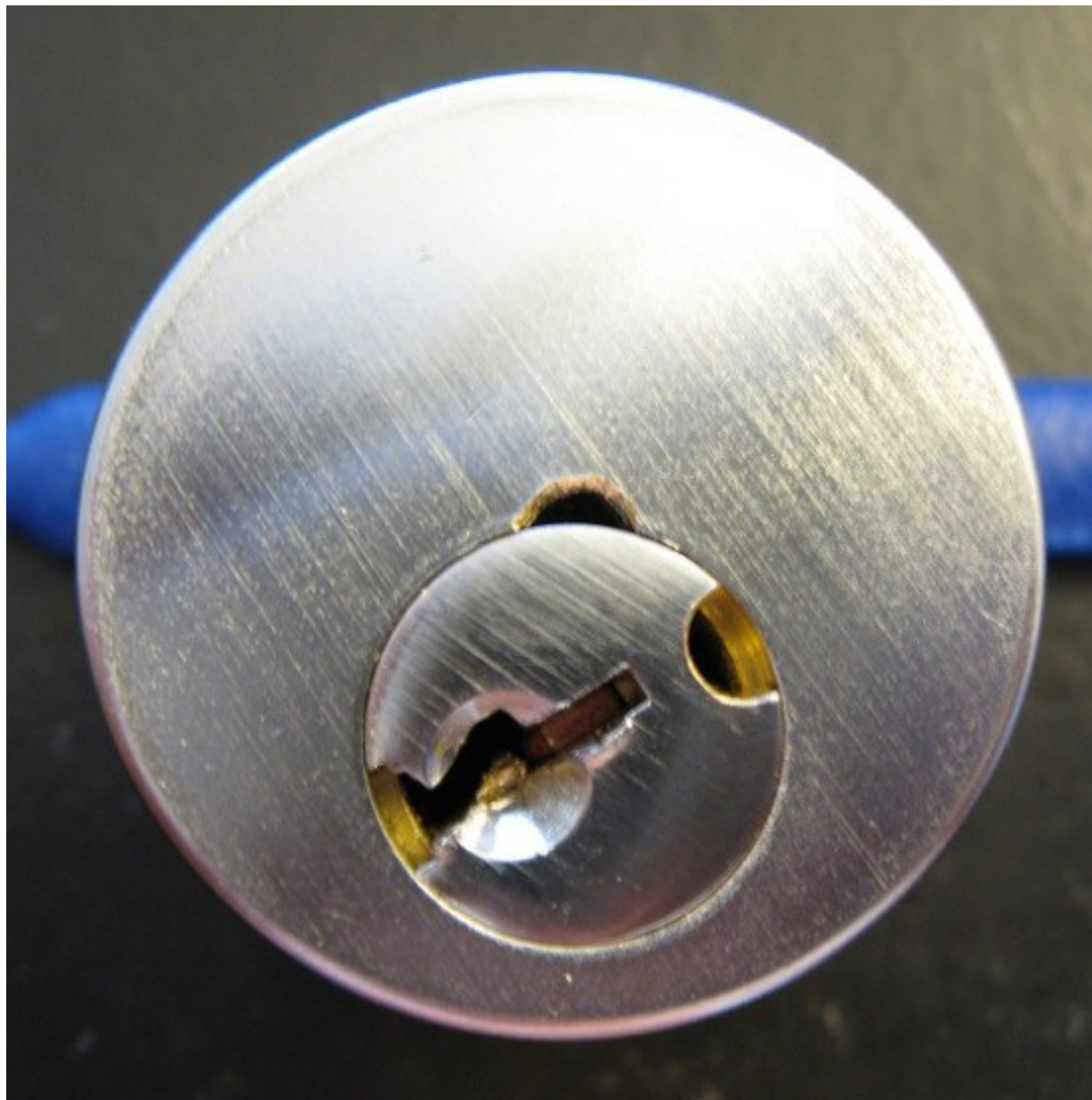
# But what about destructive entry?







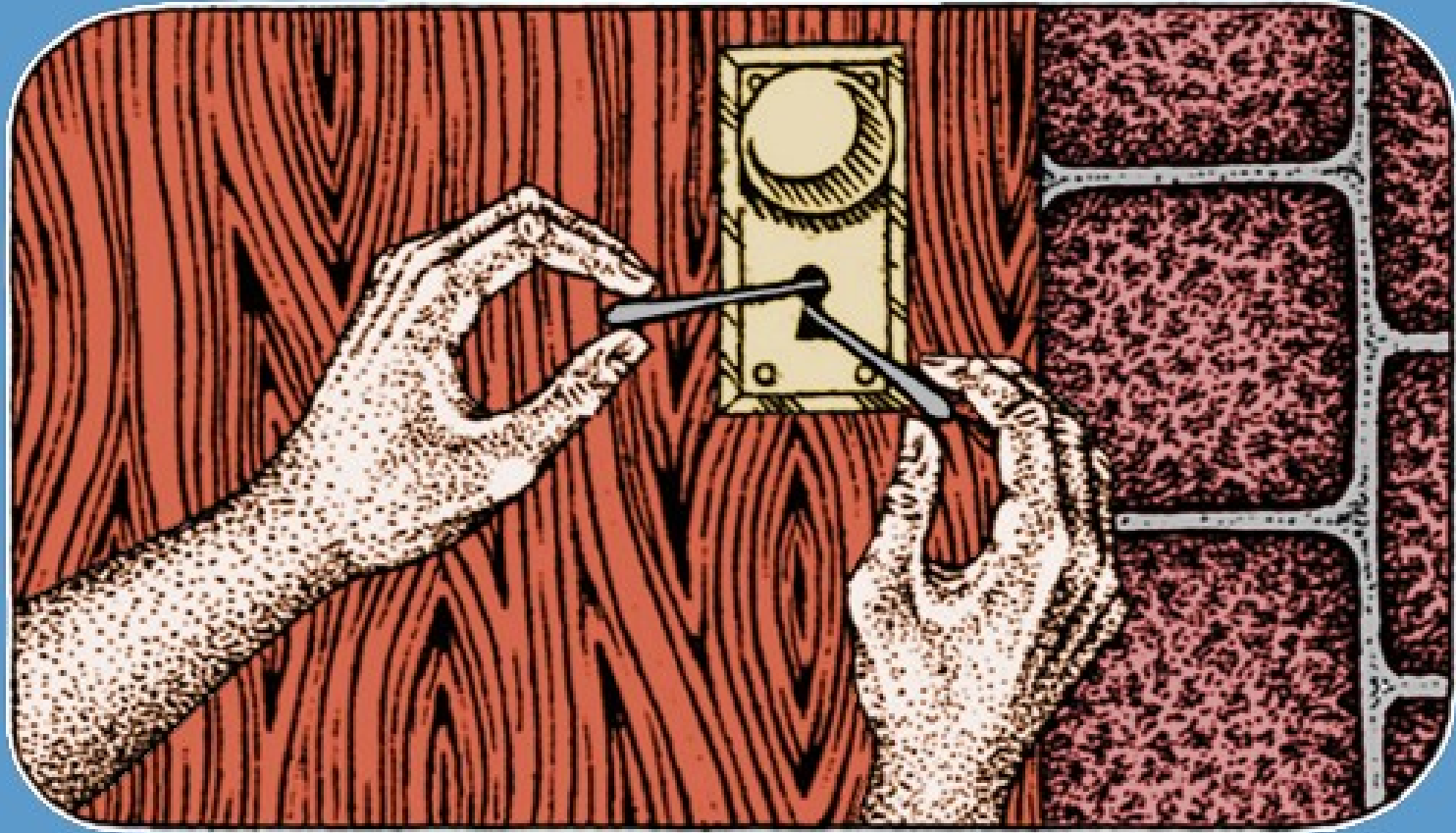




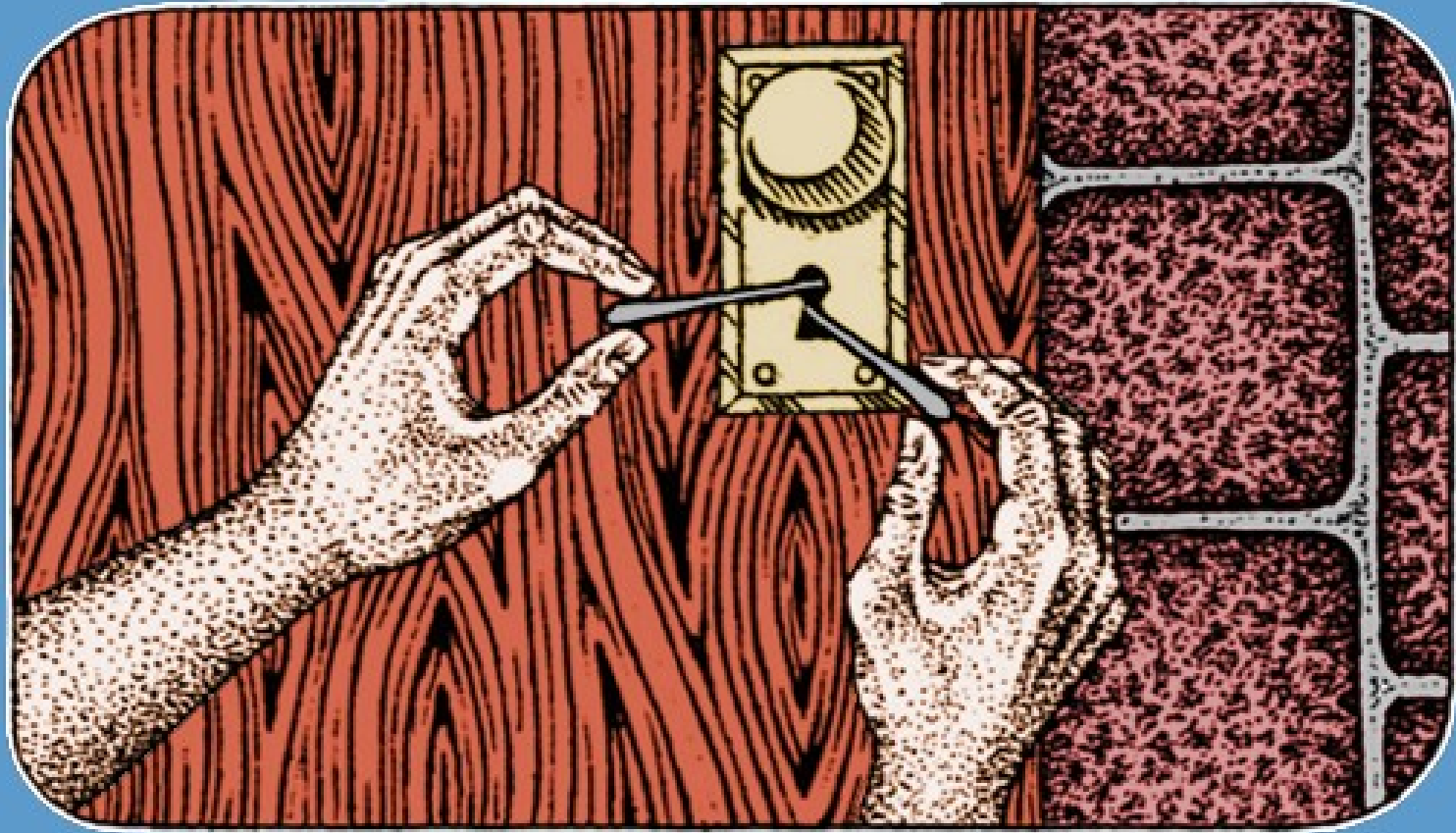




# There's one upshot... you know it happened



# The scarier risk is non-destructive entry

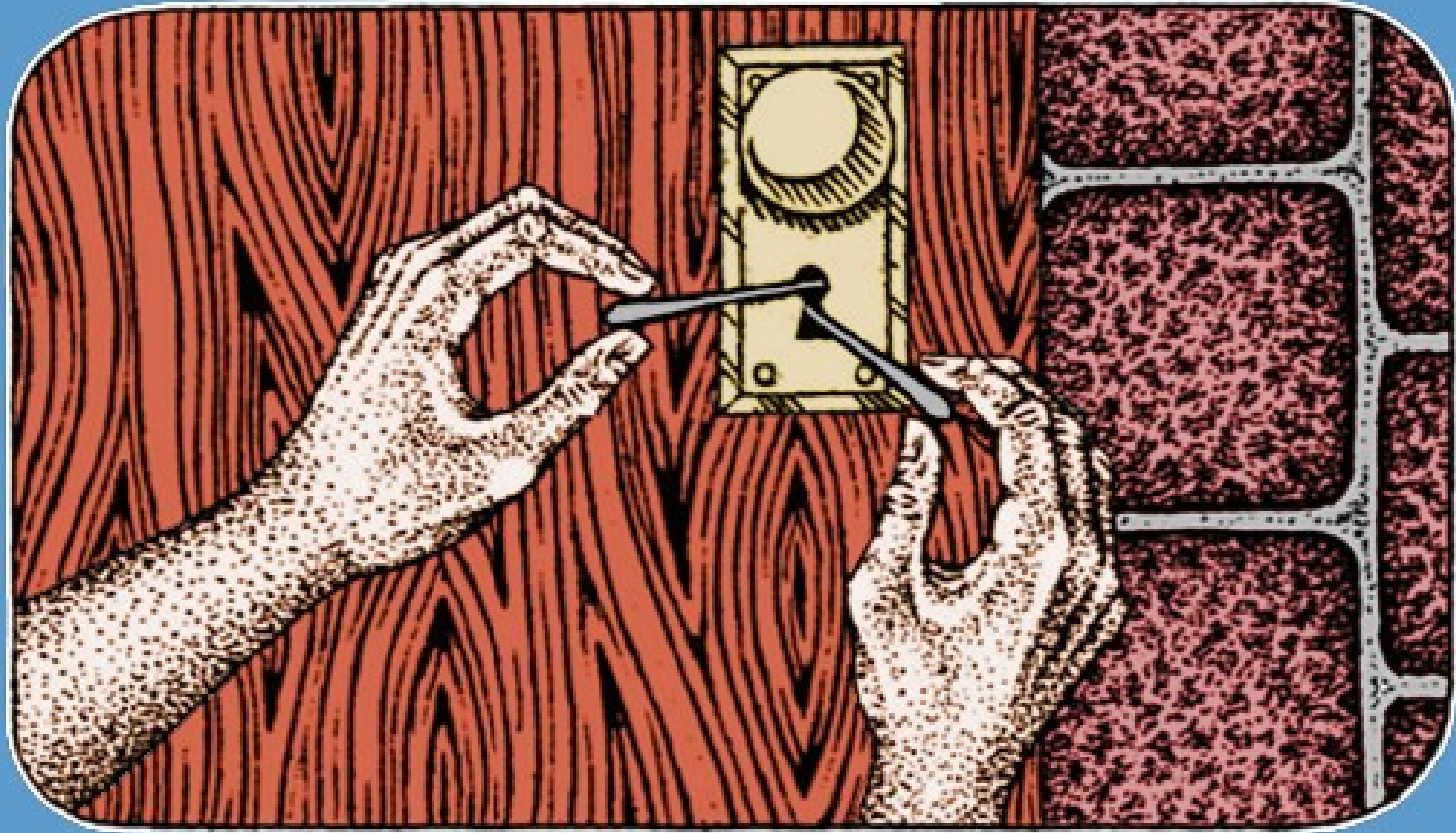








# Different locks for different purposes





# 1. Basic Locks



*No special protections*  
*No bypassing resistance*

**Unskilled Attacker - basic tools & techniques, under 5 minutes**

**Skilled Attacker - basic tools & techniques, under 5 minutes**

# 2. Resistant Locks



**Some pick-resistant pins (possibly tighter keyway)**  
**Bump resistant, Zero potential of shimming or over lifting**  
**Unskilled Attacker - basic tools & techniques, more than 5 minutes**

**Skilled Attacker - basic tools & techniques, under 5 minutes**

# 3. High Security Locks



**Advanced pick resistance, possibly wholly new mechanisms**  
**Zero potential of shimming or over lifting or bumping**  
**Unskilled Attacker - no chance in less than 30 minutes**  
**Skilled Attacker - special tools & techniques, at least 5 minutes**

# 4. “Unpickable” Locks



**Advanced pick resistance, possibly wholly new mechanisms**  
**No potential of shimming or over lifting / Bump resistance**  
**Unskilled Attacker - no chance at all**  
**Skilled Attacker - highly special tools & techniques, at least 30 minutes**

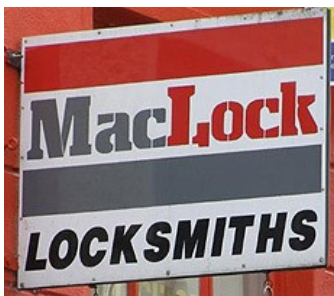








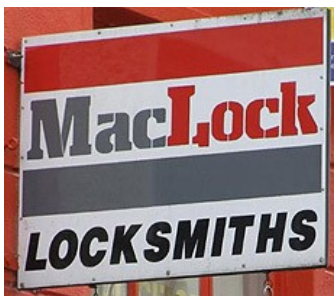








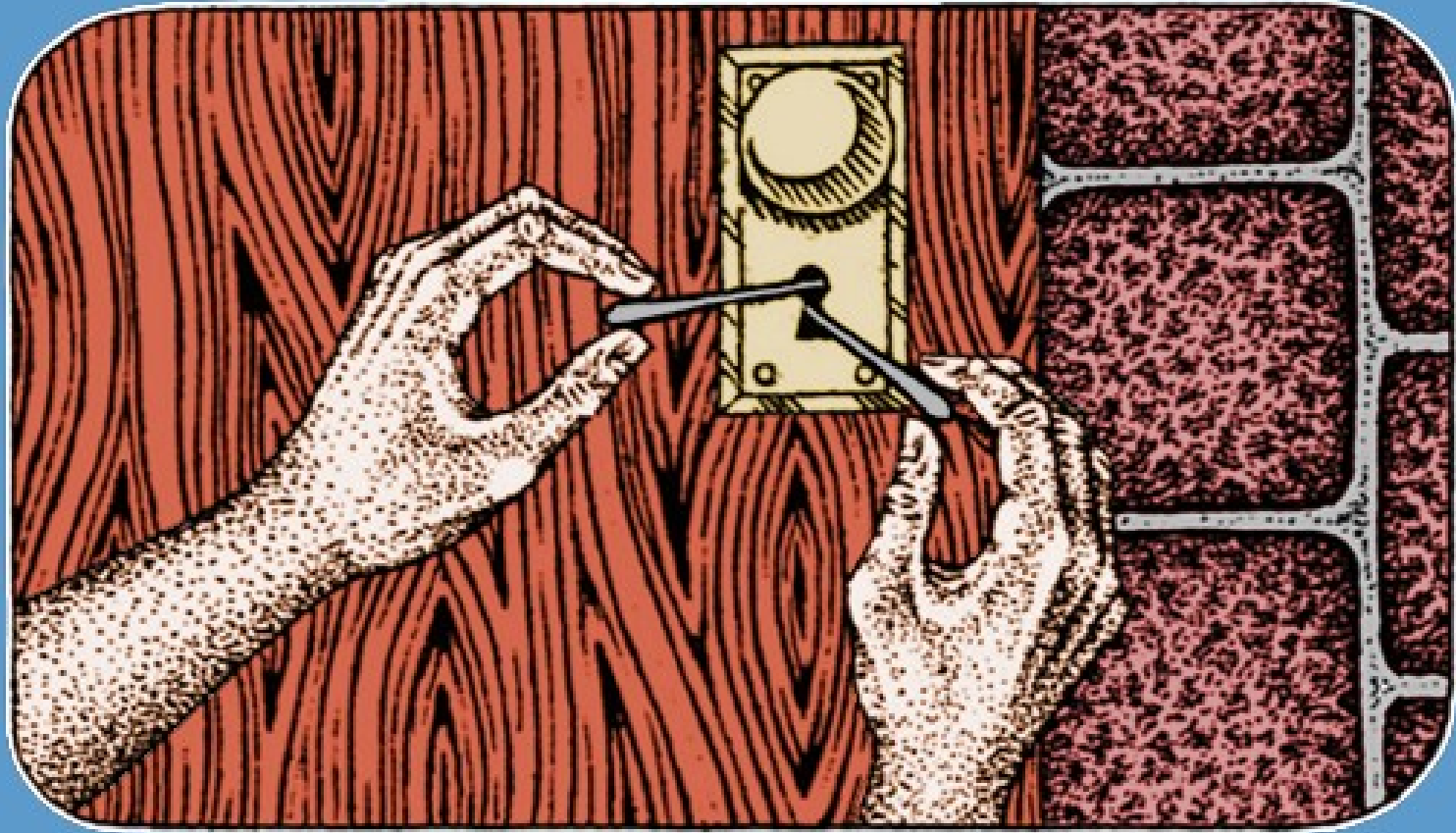








# Protecting against force or finesse?



# A New Physical Security

## Framework

- Three Types of Secured Area
  - External Access
  - Internal Access
  - Sensitive Access
- Which Locks Go Where...?



# A New Physical Security

## ● Basic Locks Framework

- Utterly unacceptable
- Should be *removed*, in my view
- False sense of security
- Inevitable “cross-contamination”





# “Cross Contamination”



# **“Cross Contamination”**

## **with Locks**





# “Cross Contamination”

■ ■ ■ ■ ■



# “Cross Contamination”



# “Cross Contamination”





# “Cross Contamination”





# “Cross Contamination”



# A New Physical Security

## ● Basic Locks Framework

- Utterly unacceptable
- Should be *removed*, in my view
- False sense of security
- Inevitable “cross-contamination”





# A New Physical Security

## Framework

- **External Access**
  - Personnel Doors
  - Wiring / Utilities
  - Susceptible to Vandals & Thugs
- **High Security Locks Should Be Required**



# A New Physical Security

- **Internal Access Framework**
  - Office Doors
  - Closets
  - Protecting Privacy & Supplies, not Data
- **Pick Resistant Locks Are Acceptable**



# A New Physical Security

## Framework

- Sensitive Access
  - Server Racks
  - Networking Equipment
  - Any Termination-Worthy Data
- **“Unpickable” Locks Should Be Used**



# To Me, a “Proper” Lock Should...

- ✓ Be Totally Immune to Zero-Skill Attacks
- ✓ Resist Skilled Tactics for Thirty Minutes
- ✓ Leave Behind Clear Signs of Tampering



# Security is only as effective





# Social Engineering



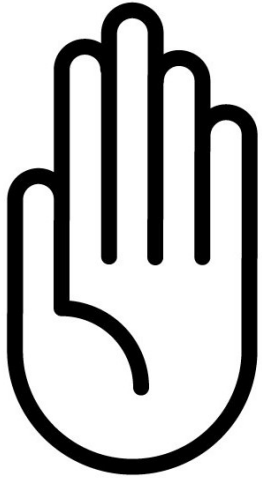
# Social Engineering



# Social Engineering



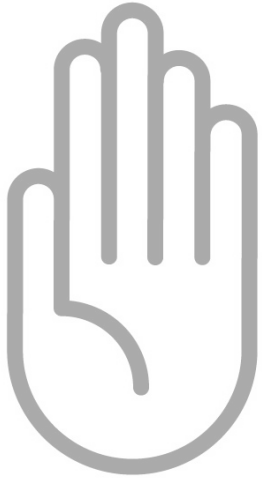
# Social Engineering Preparedness



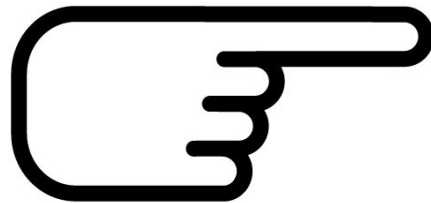
**Stop**

# Social Engineering

## Preparedness



**Stop**



**Challenge**



# Social Engineering

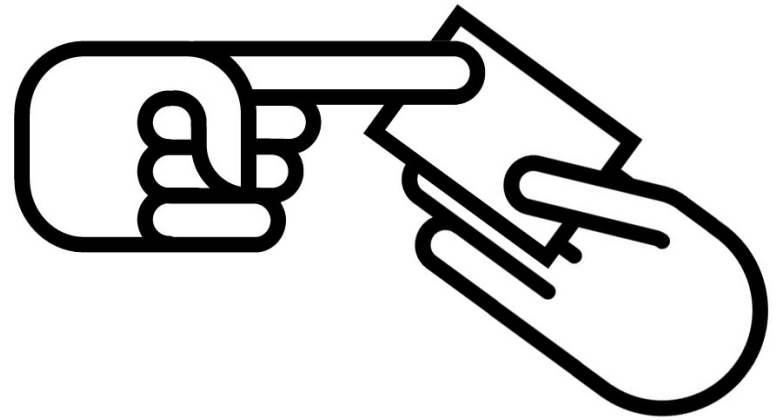
## Preparedness



**Stop**



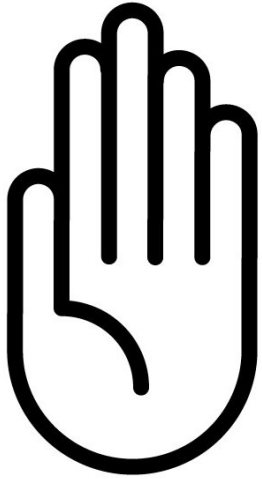
**Challe  
nge**



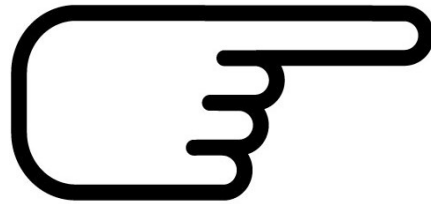
**Authenti  
cate**

# Social Engineering

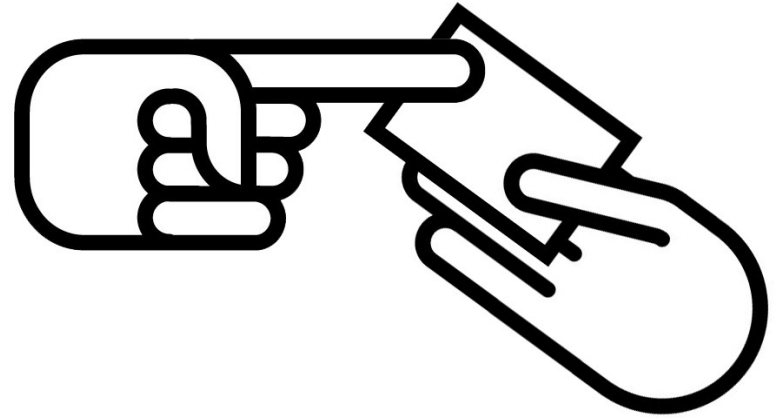
## Preparedness



**Stop**



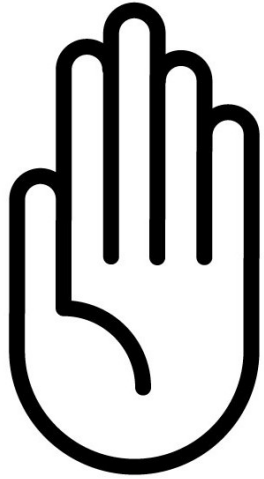
**Challe  
nge**



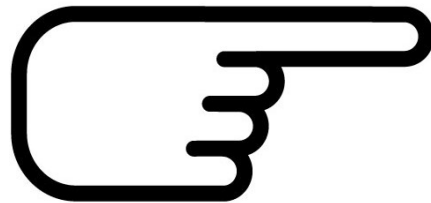
**Authenti  
cate**

# Social Engineering

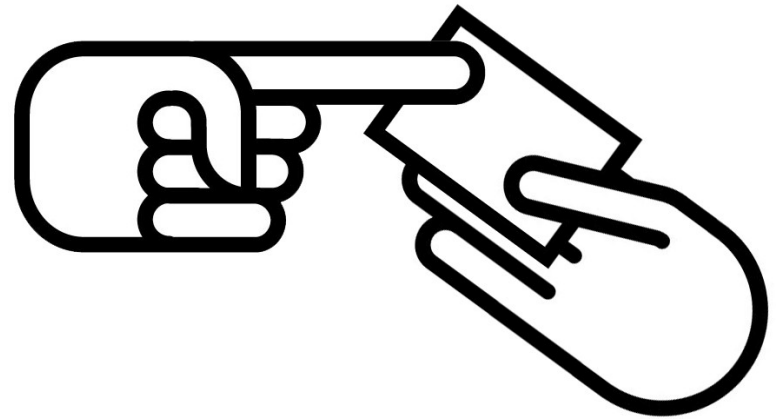
## Preparedness



**Stop**



**Challe  
nge**



**Authenti  
cate**

**... then you follow this  
with “Reward”**

# Social Engineering



# Social Engineering

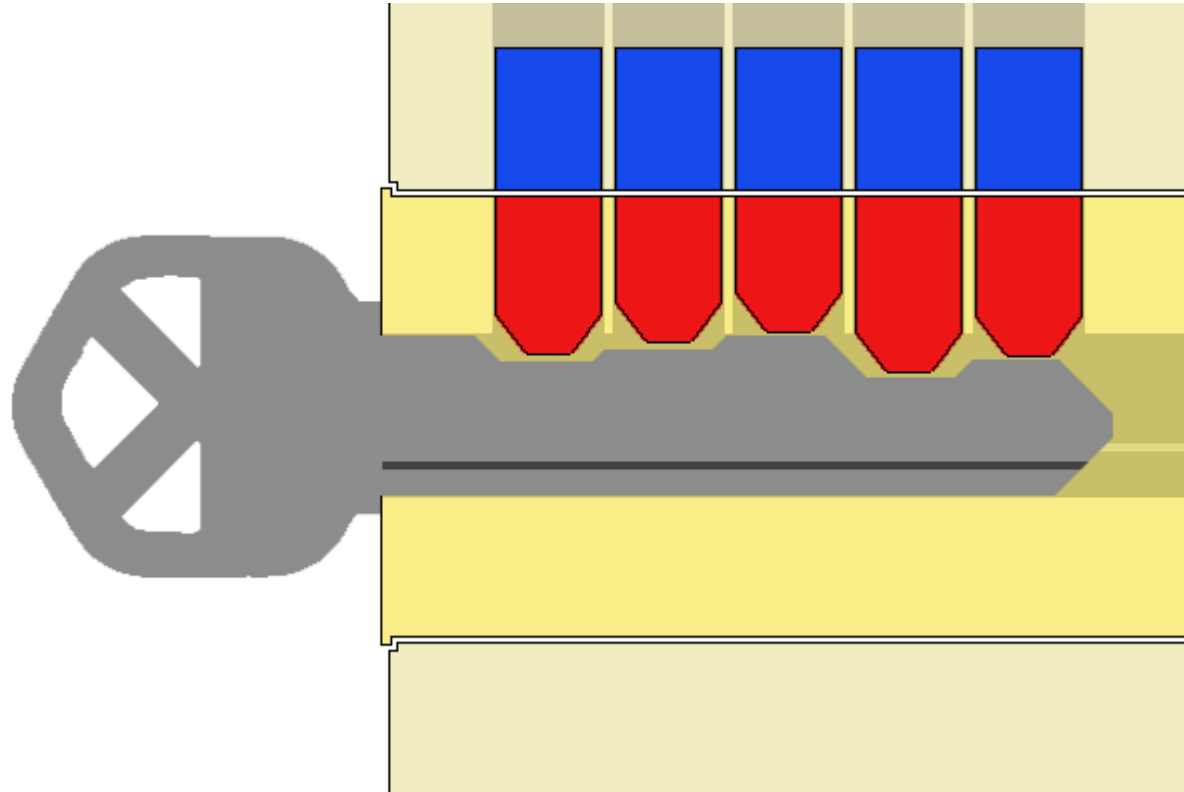




# Forensic Evidence



# Forensic Evidence



# Forensic Evidence



# Forensic Evidence



# Forensic Evidence - 250 uses





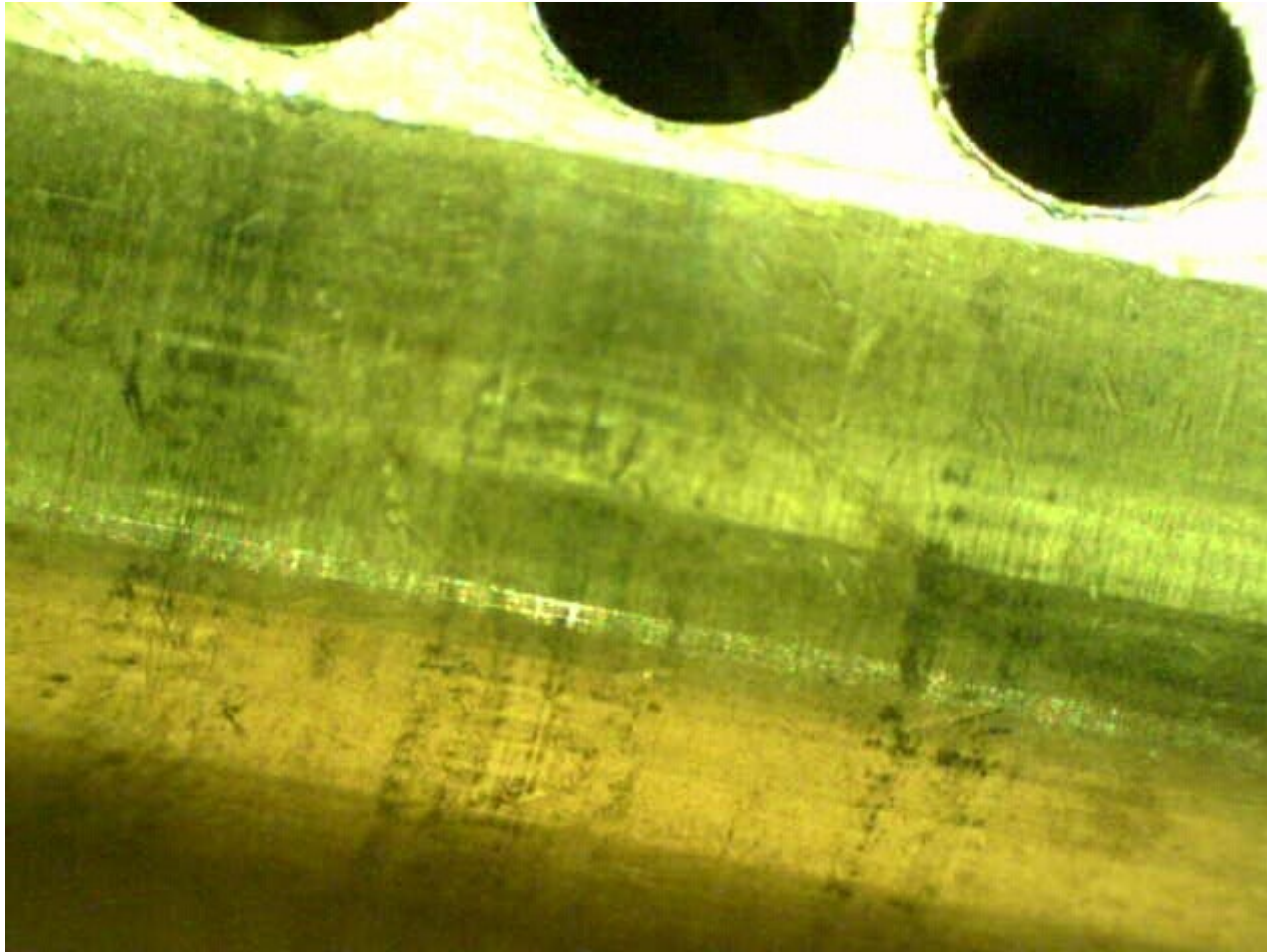
# Forensic Evidence - 1,500 uses



# Forensic Evidence - 5,000 uses

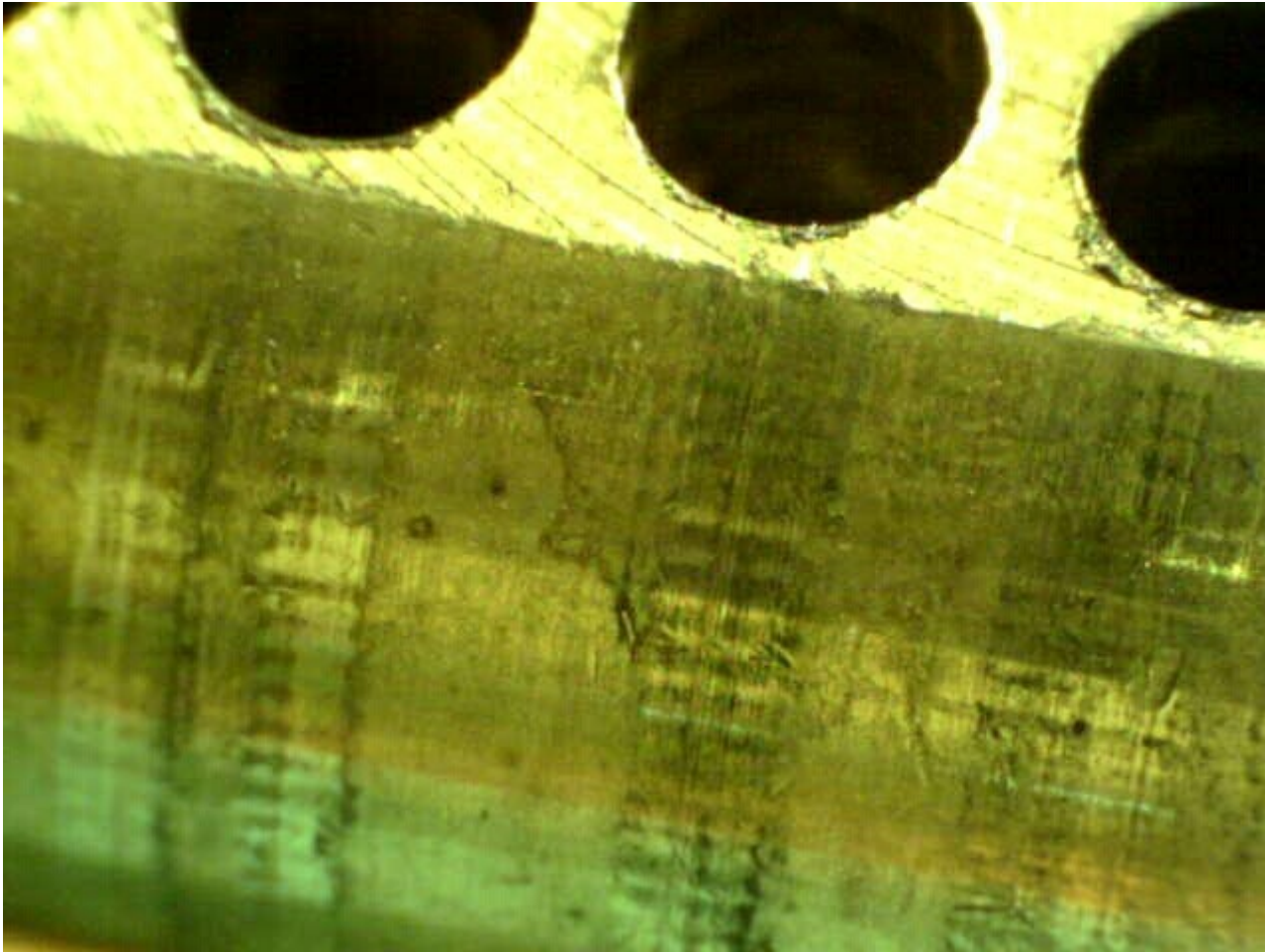


# Forensic Evidence - 250 uses

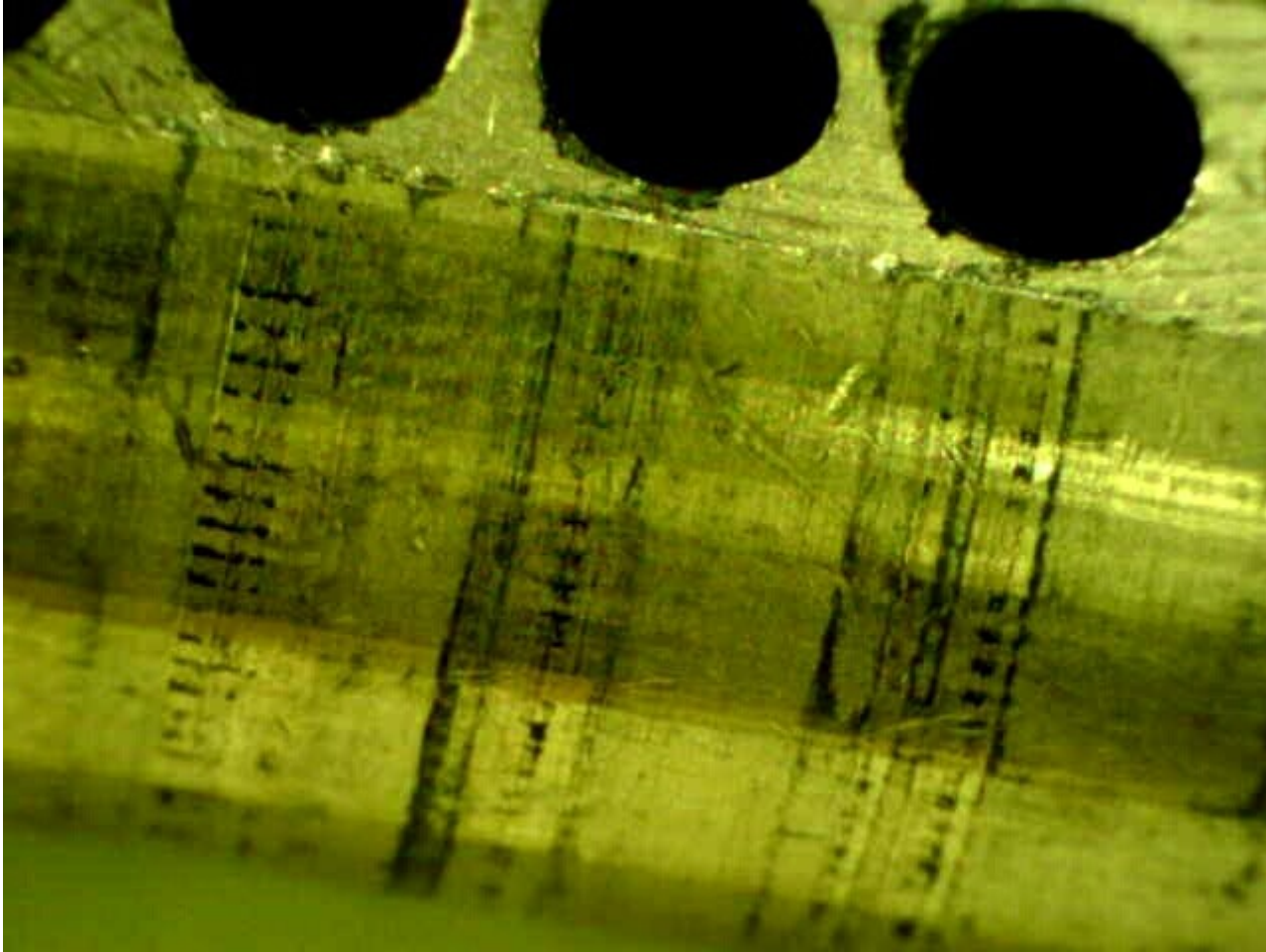




# Forensic Evidence - 1,500 uses

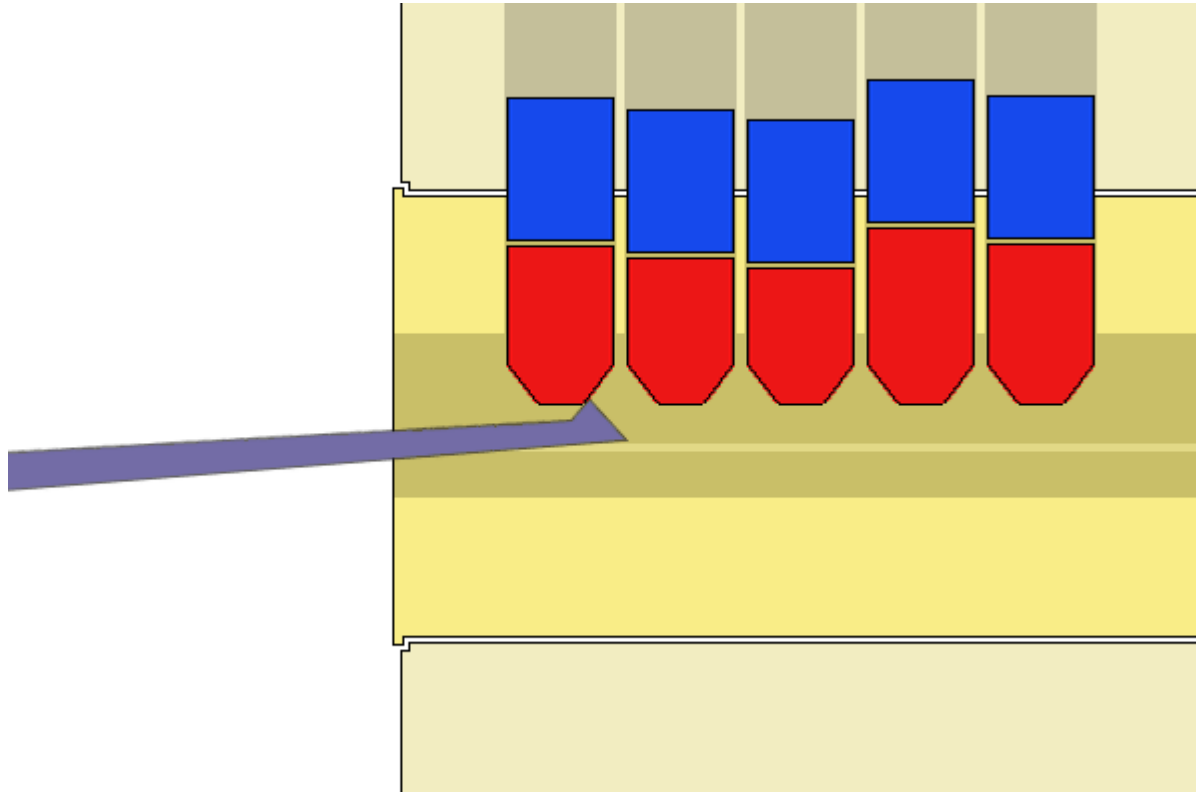


# Forensic Evidence - 5,000 uses





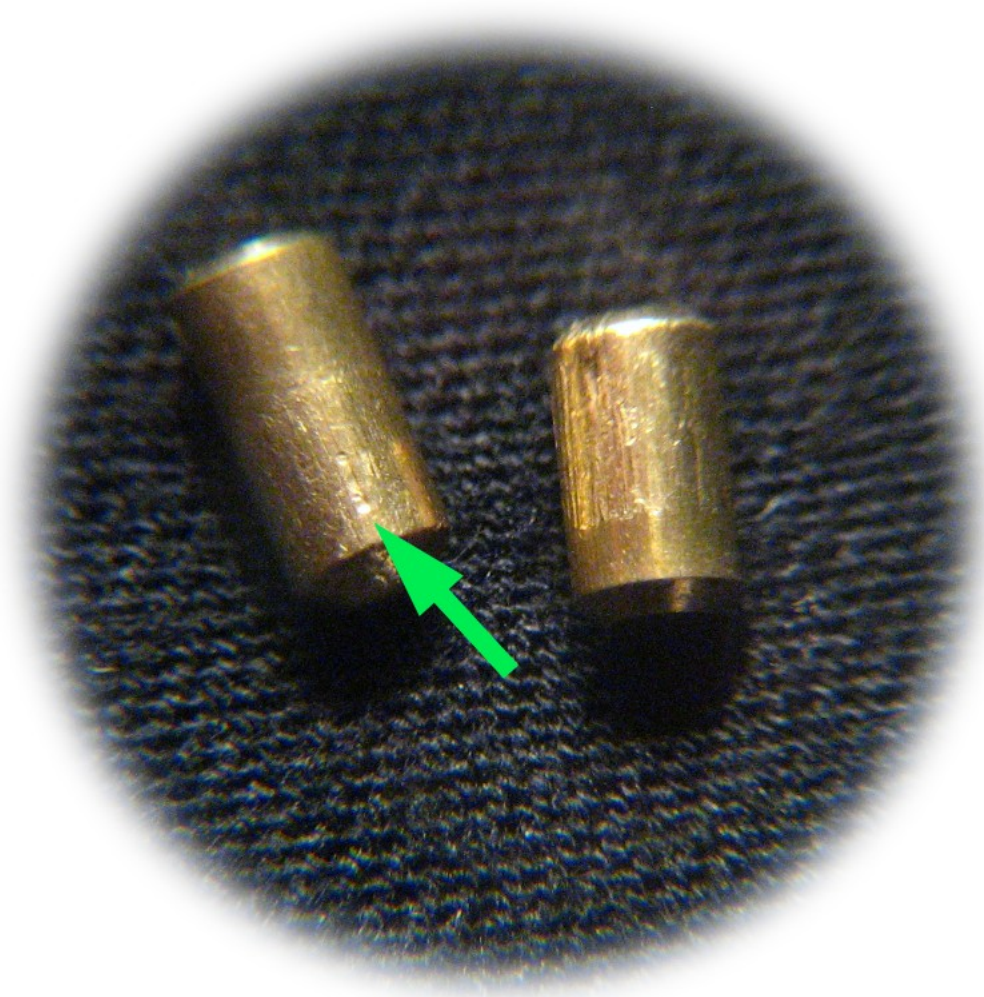
# Forensic Evidence



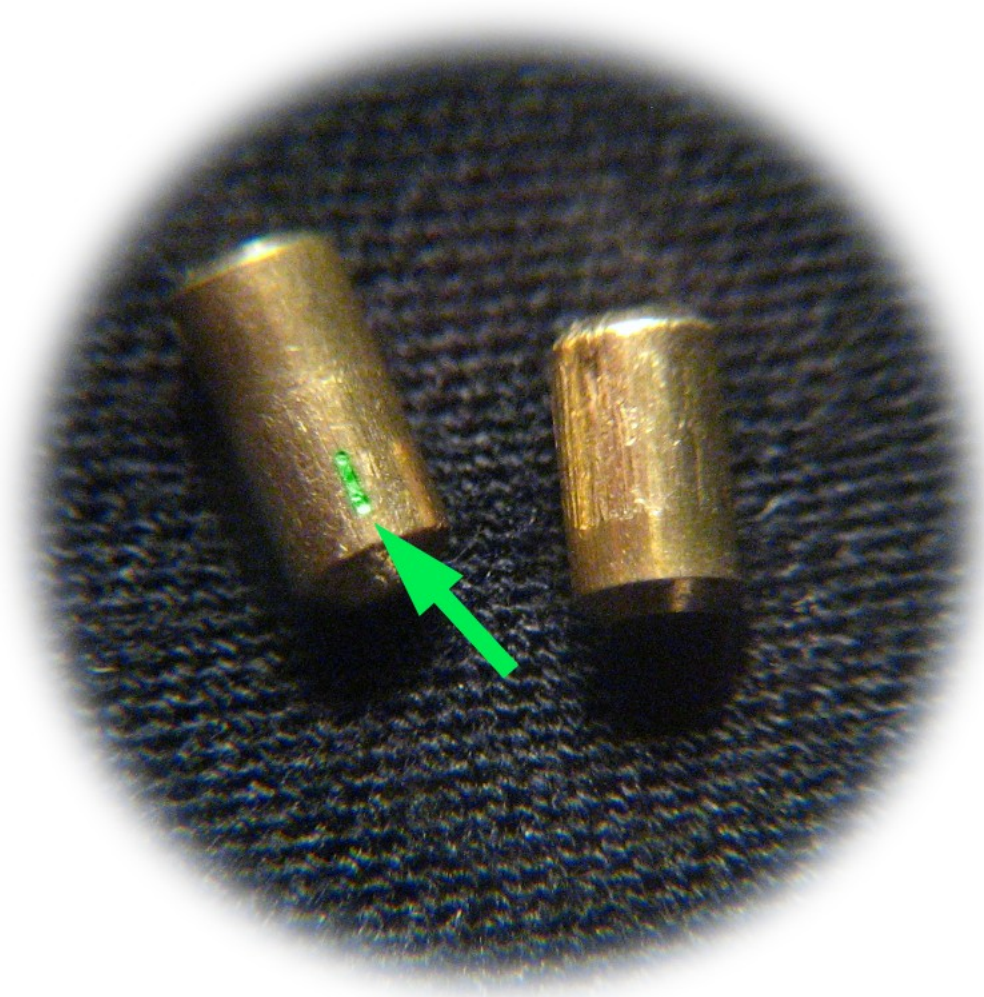
# Forensic Evidence



# Forensic Evidence



# Forensic Evidence





# Forensic Evidence





# Forensic Evidence - picking



# Forensic Evidence - raking





# Forensic Evidence - both



# Forensic Evidence - ugh

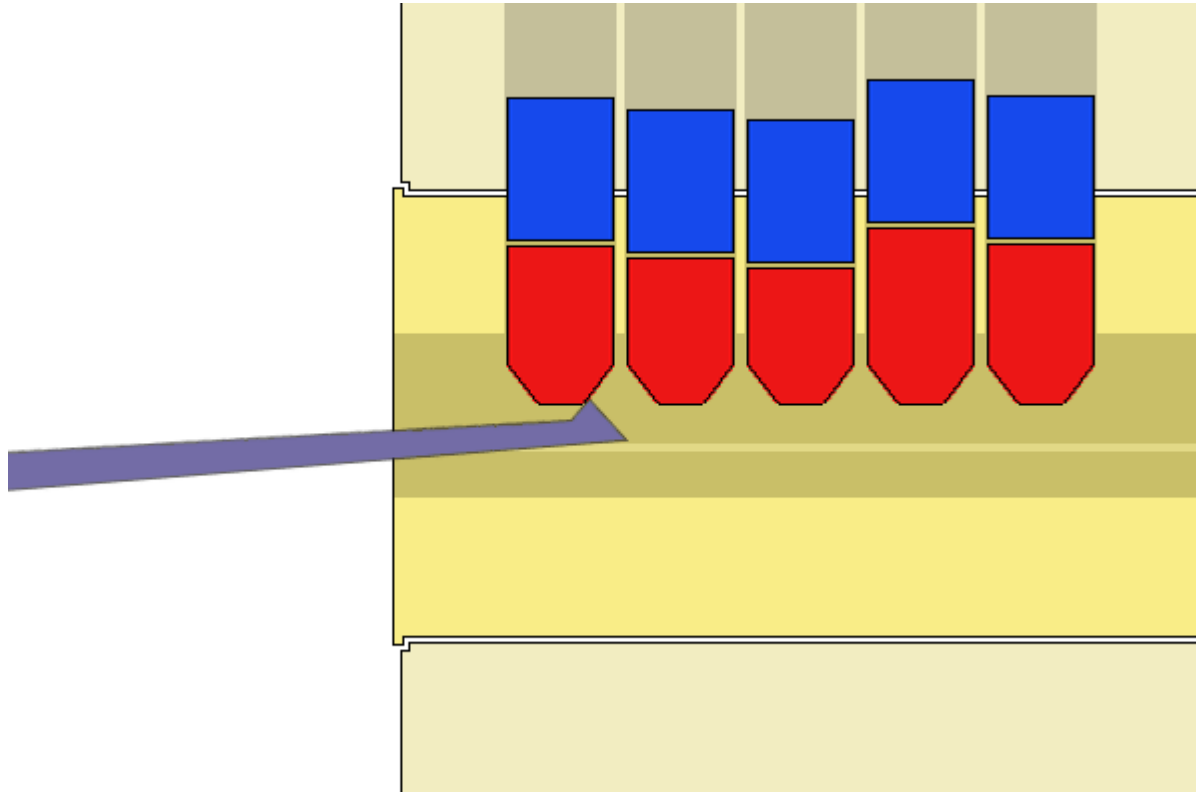


# Forensic Evidence - wow

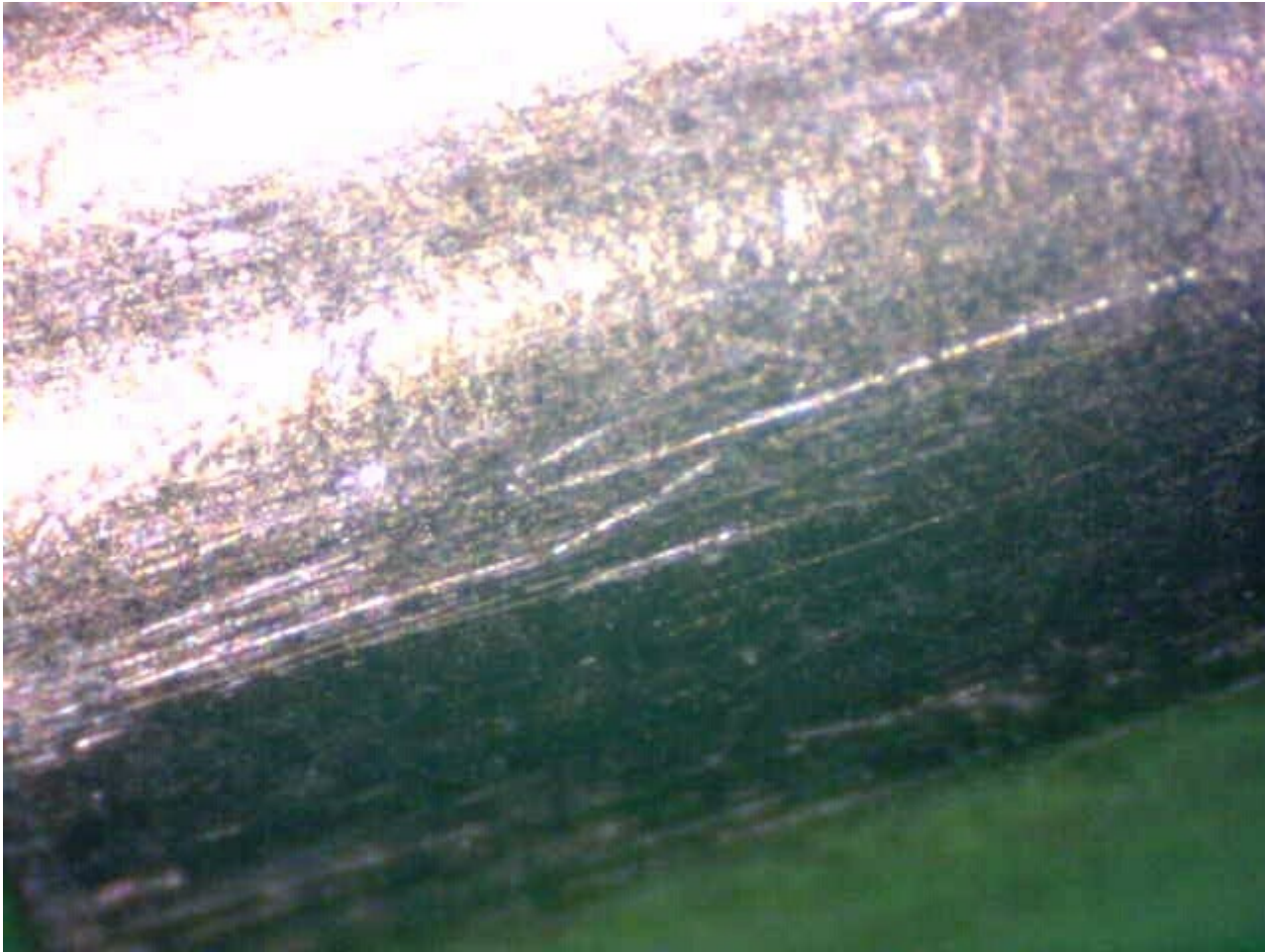




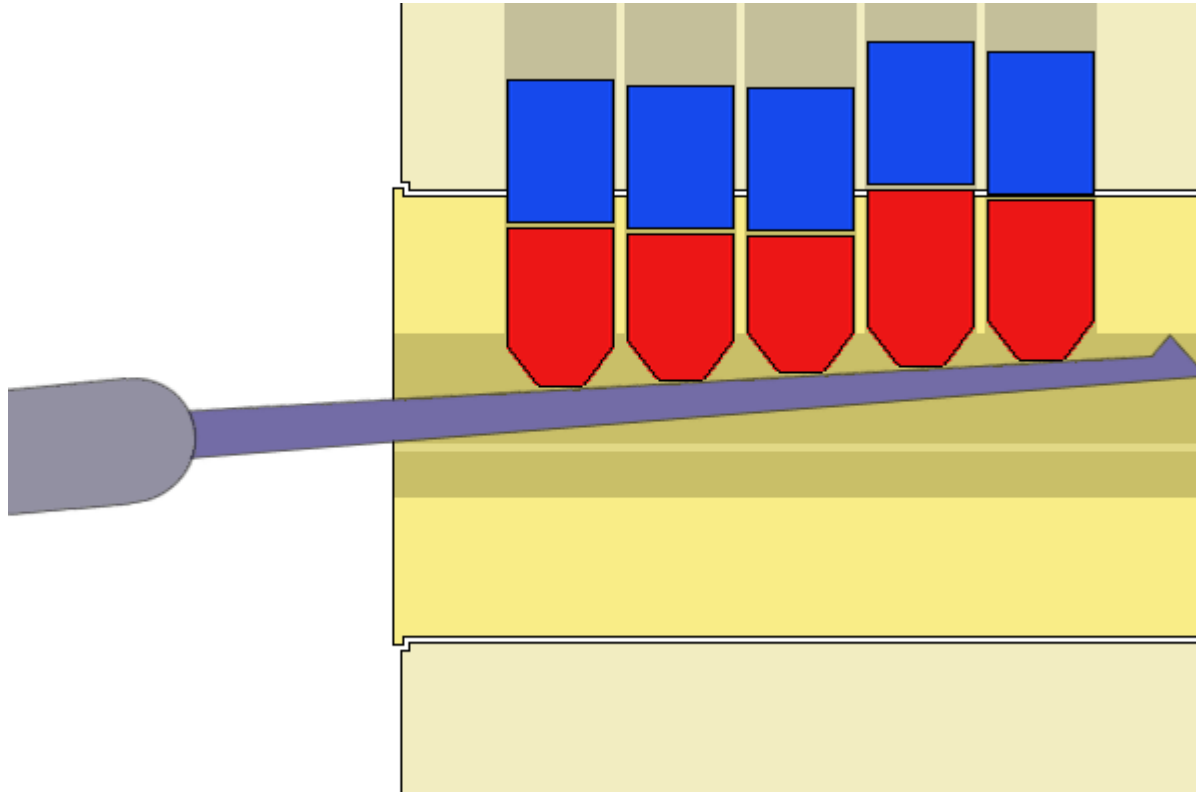
# Forensic Evidence



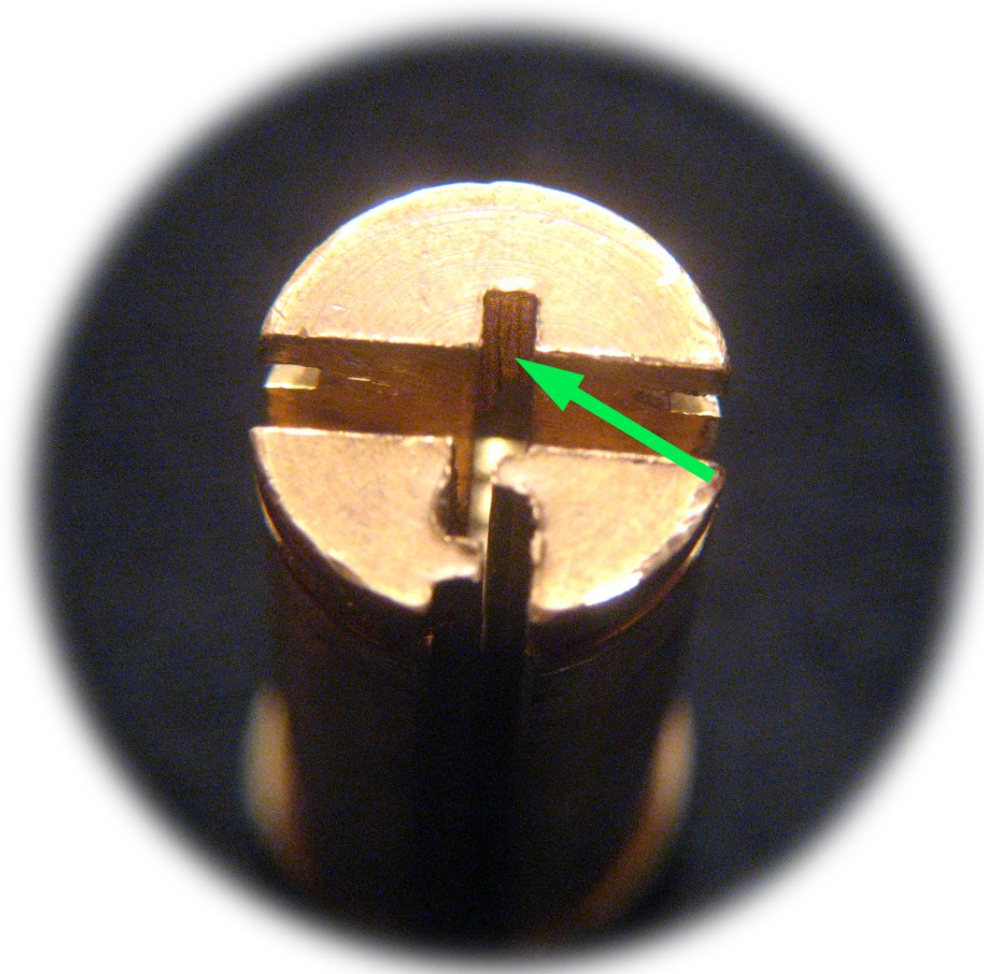
# Forensic Evidence - pin sides



# Forensic Evidence

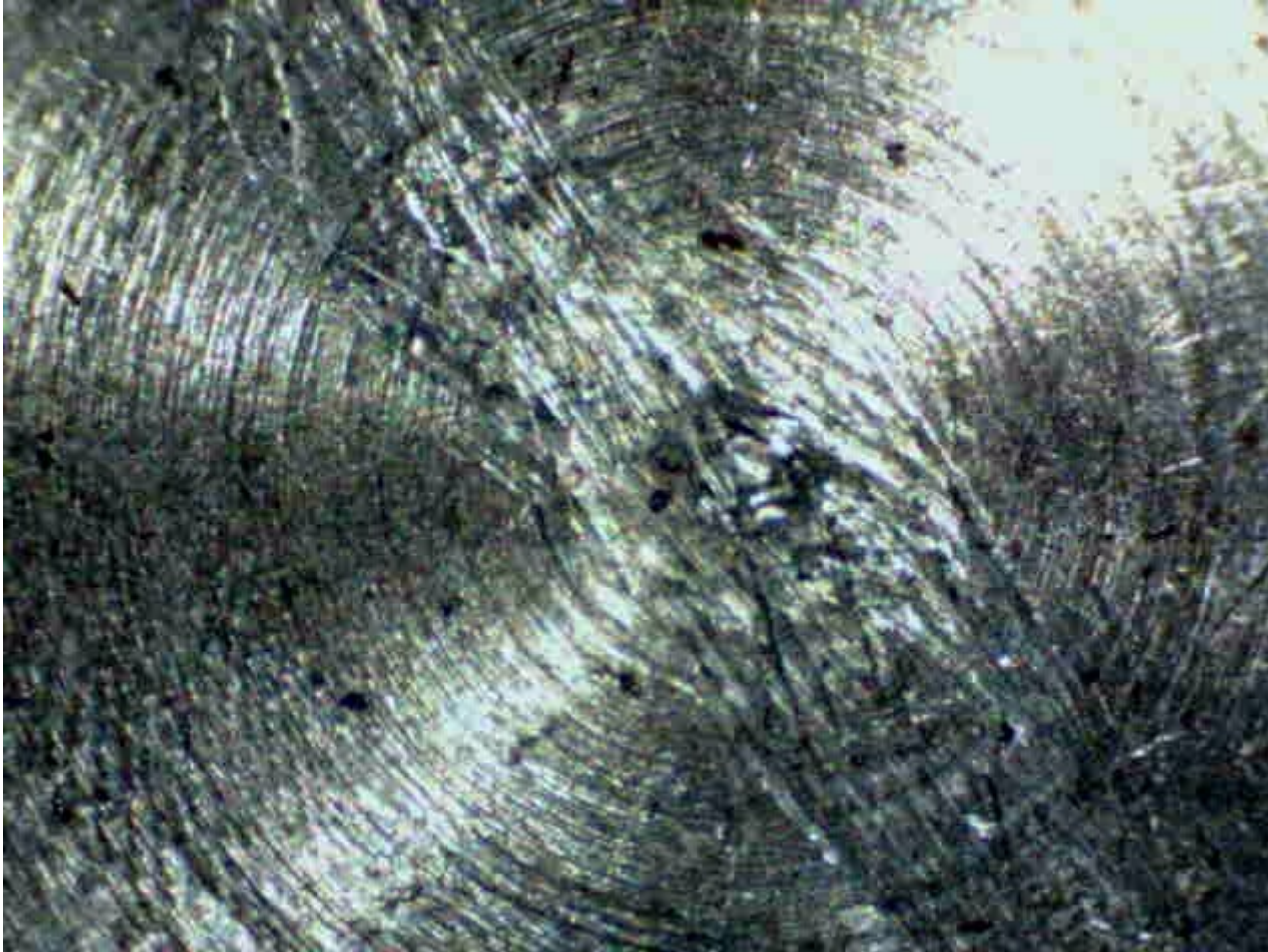


# Forensic Evidence



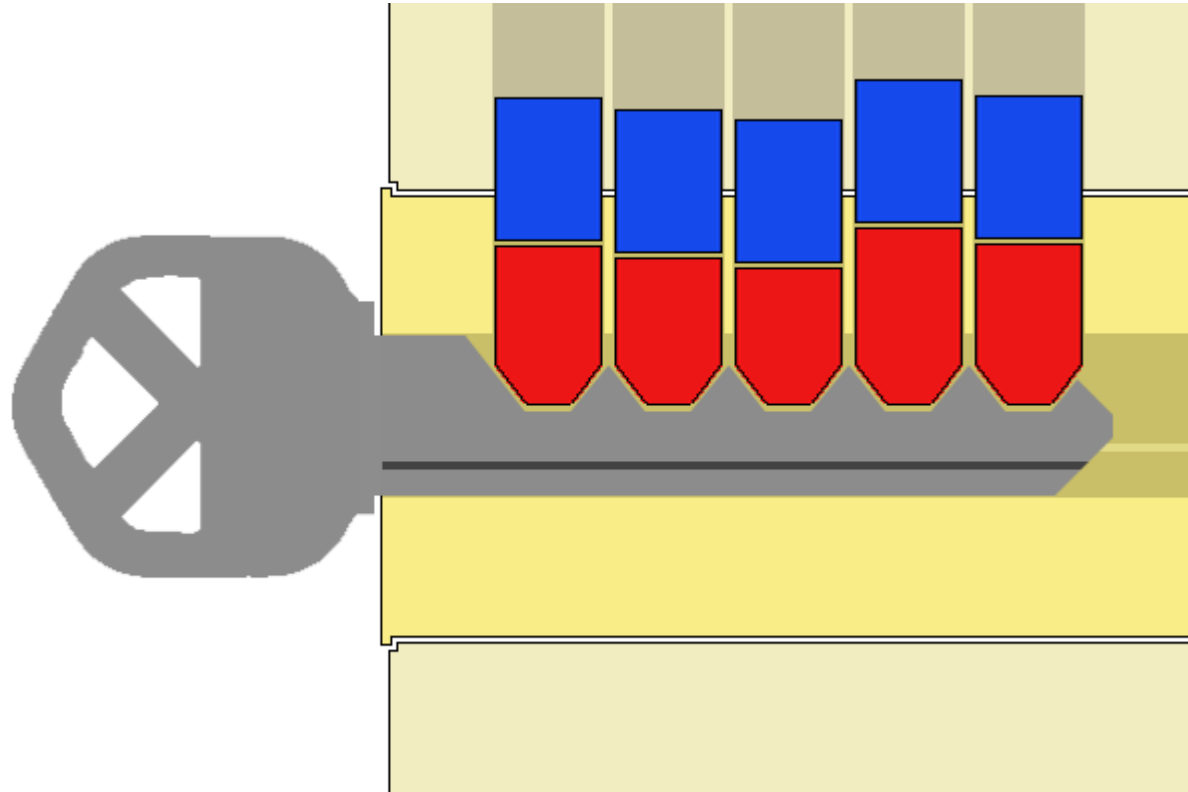


# Forensic Evidence - tail cam

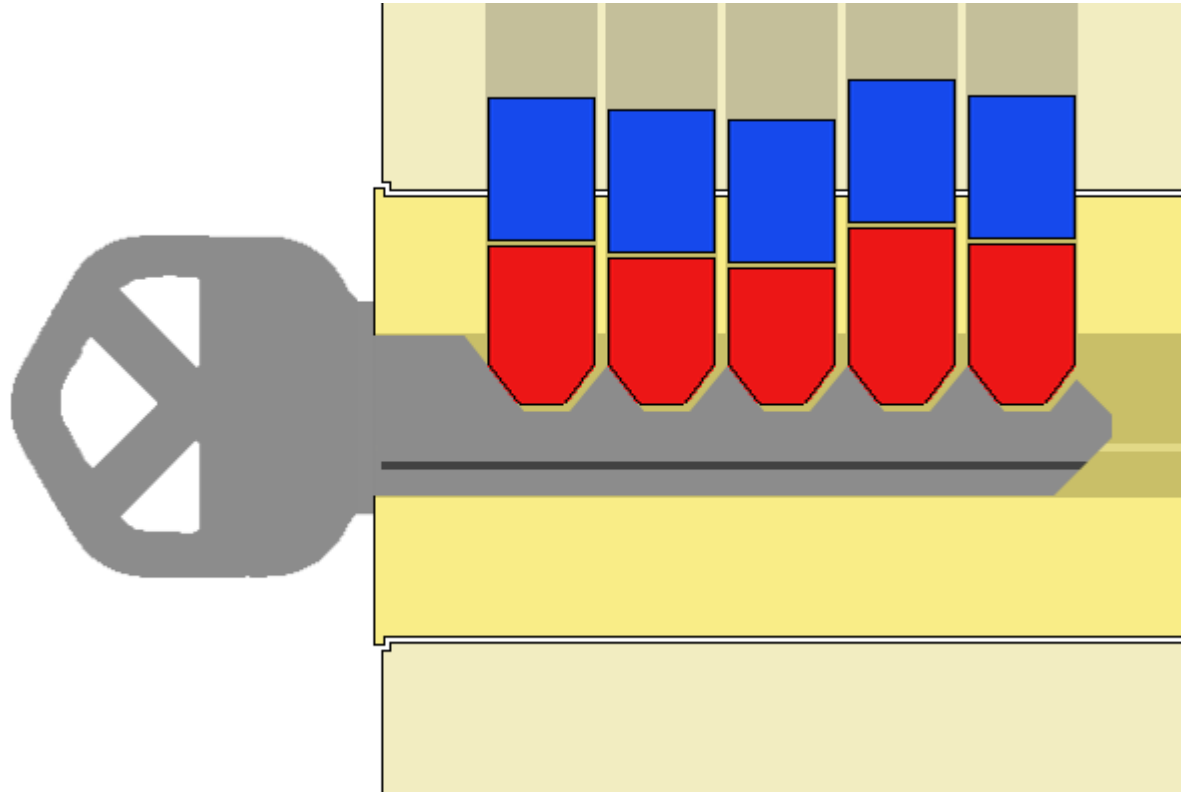




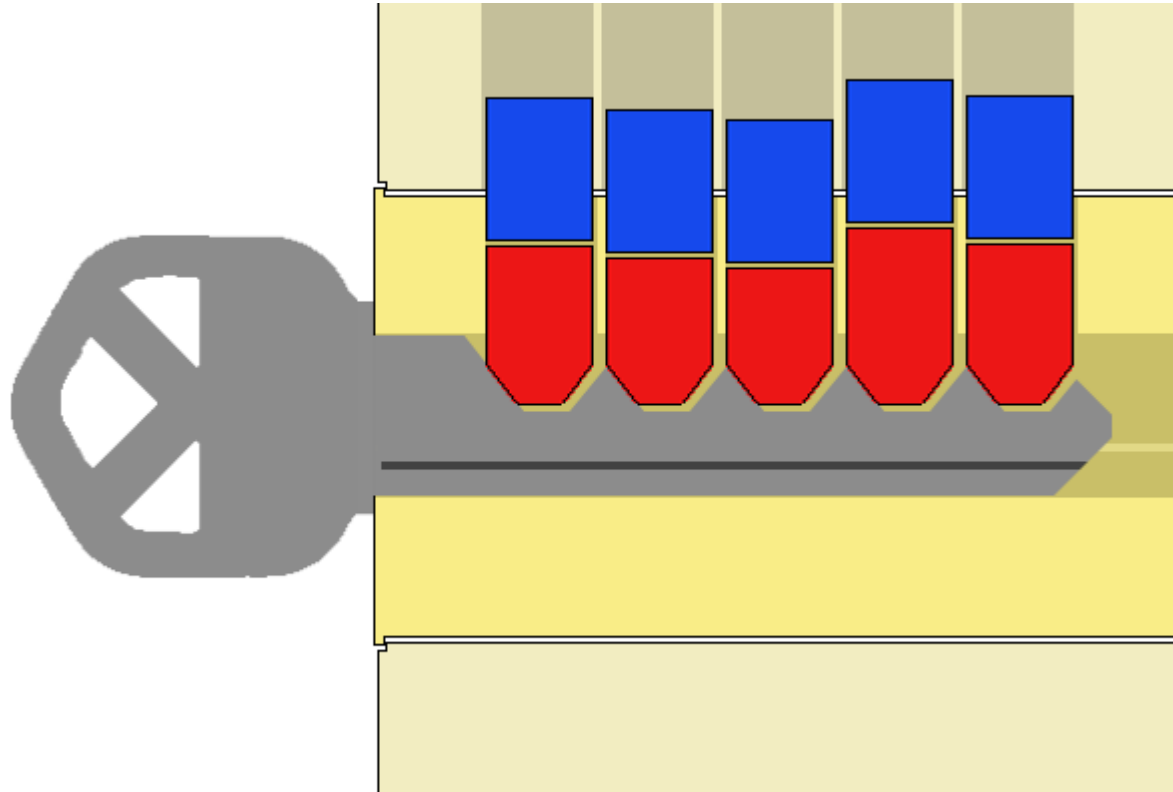
# Forensic Evidence



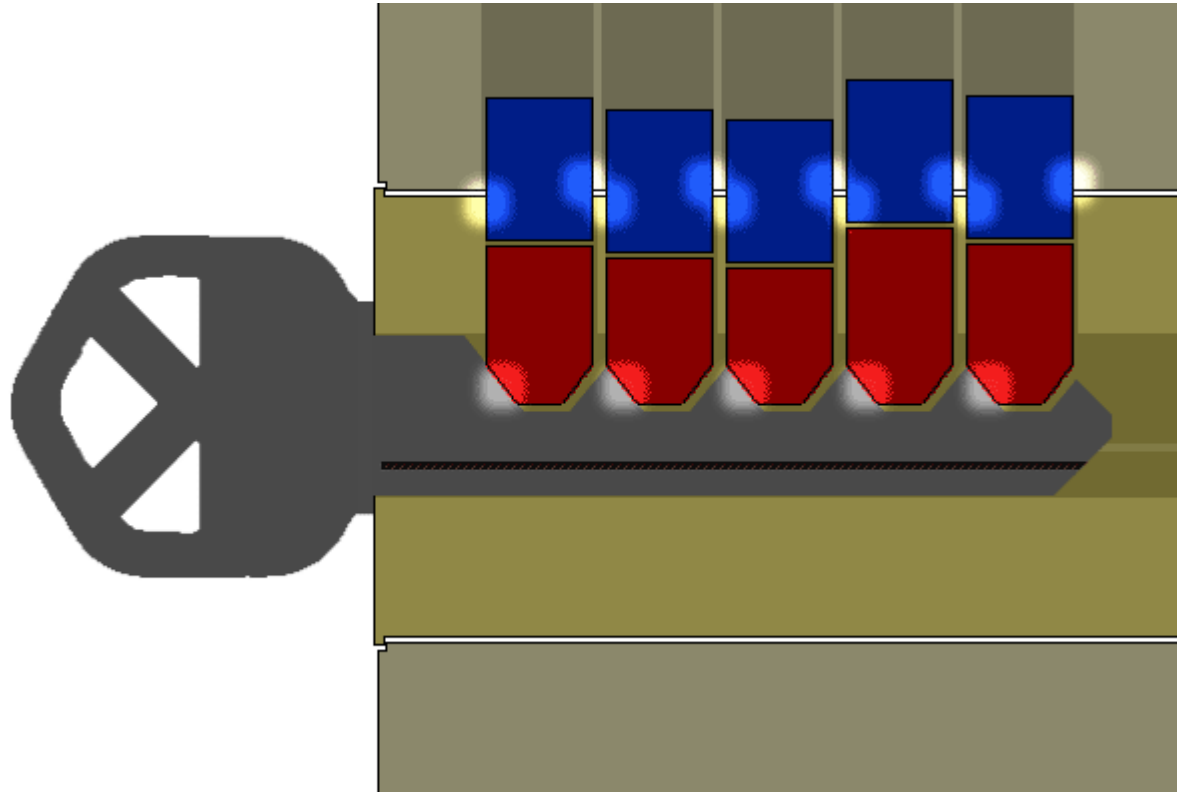
# Forensic Evidence



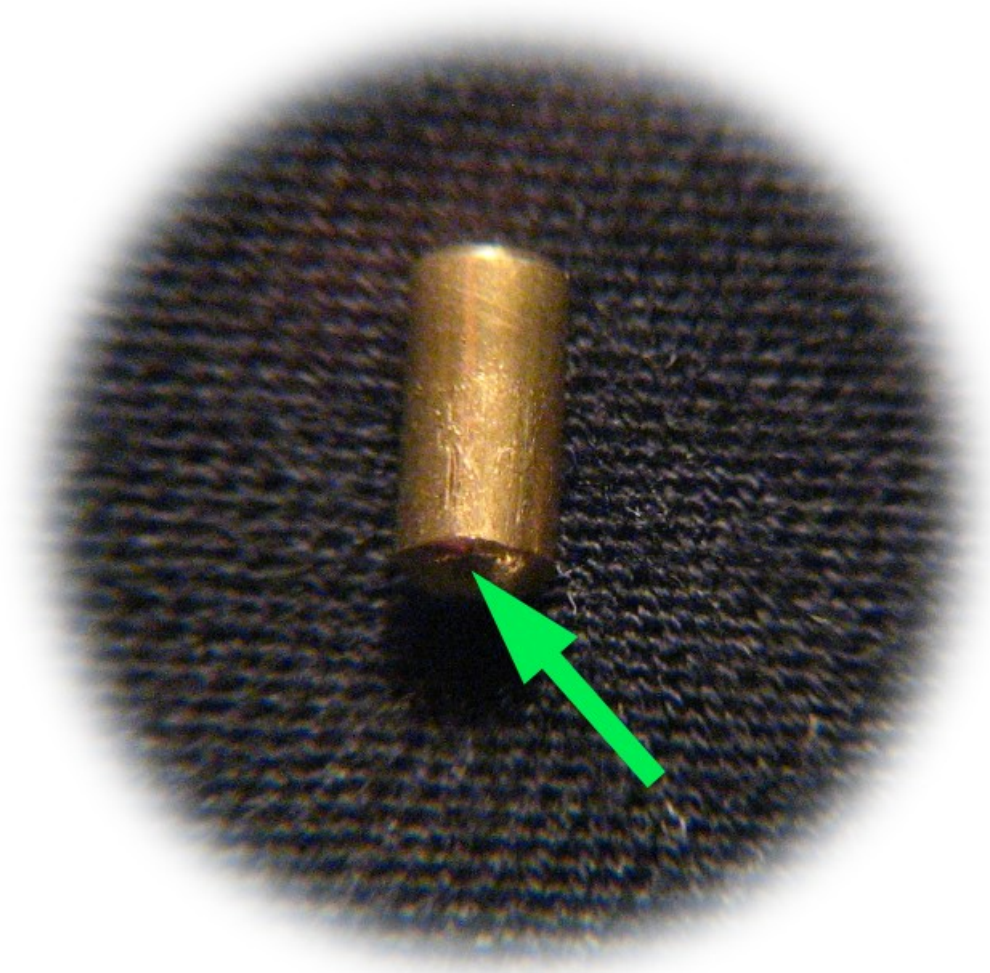
# Forensic Evidence



# Forensic Evidence

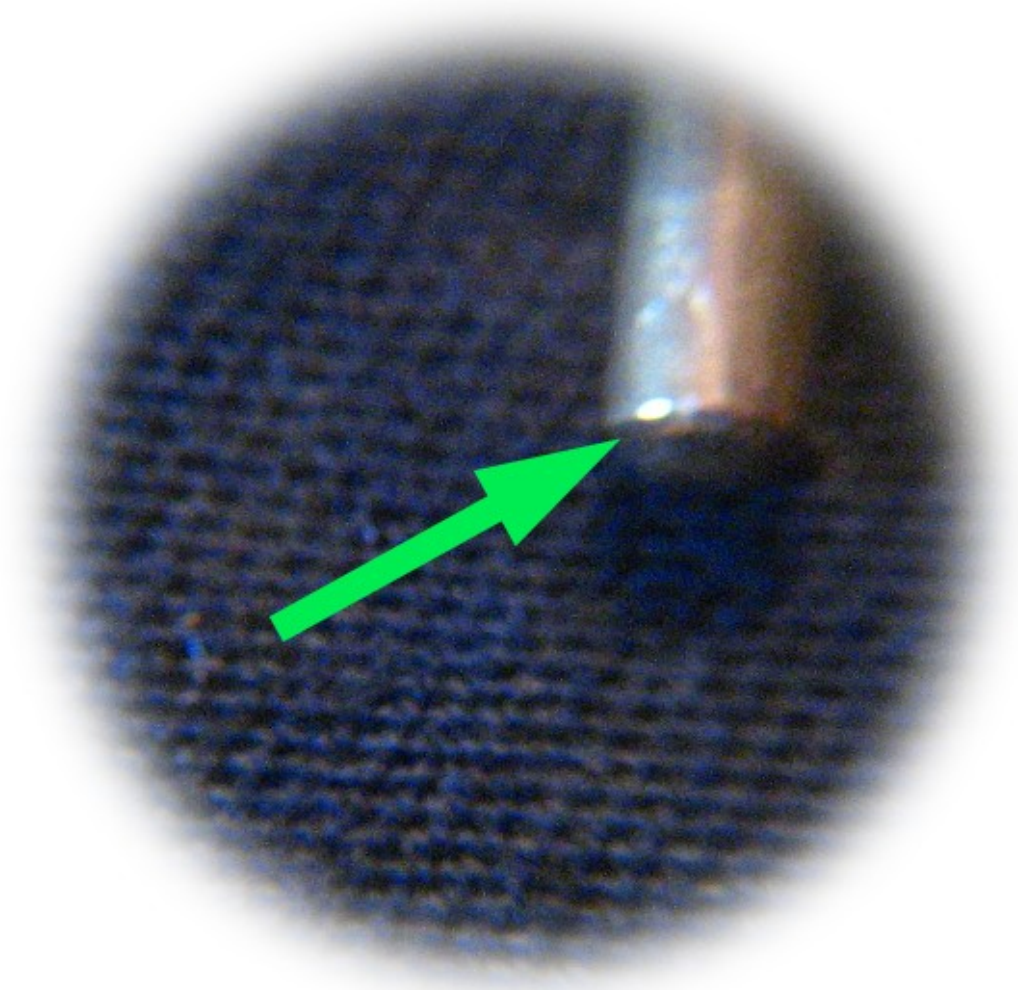


# Forensic Evidence





# Forensic Evidence



# Forensic Evidence - bumping

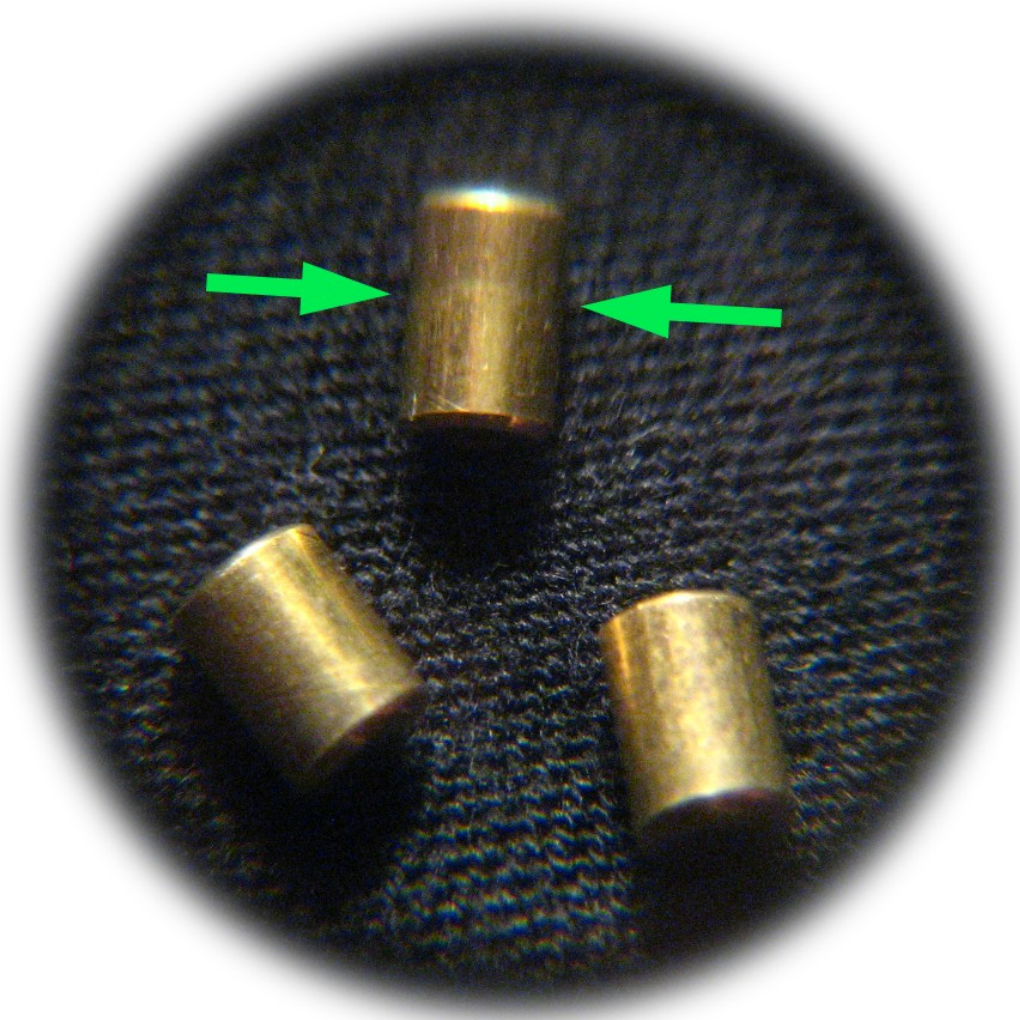


# Forensic Evidence - bumping

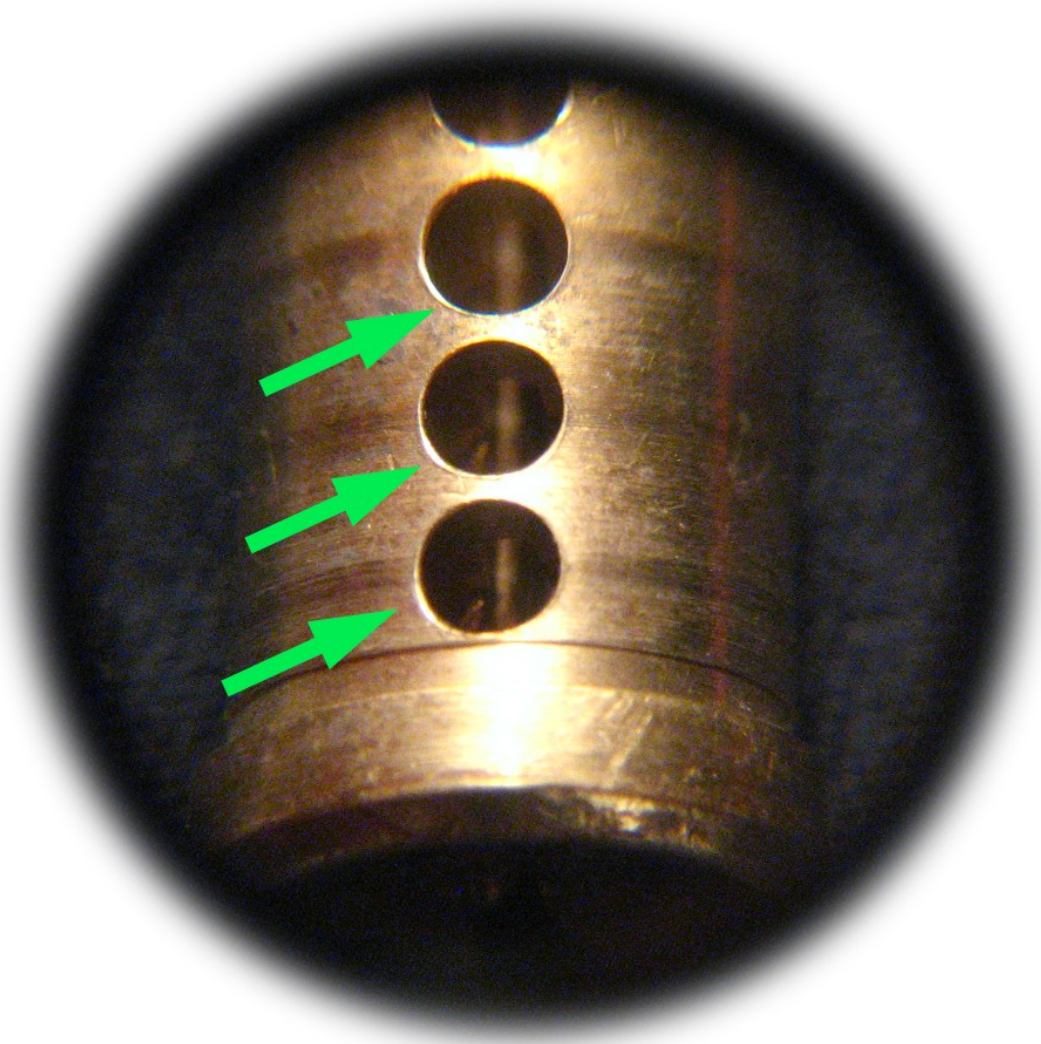




# Forensic Evidence



# Forensic Evidence





# Forensic Evidence







# Forensic Evidence





- **Sometimes *major* insurance implications**
- **Suspect something fishy?**
  - Don't compromise the scene
  - Contact a professional
  - Forensic Locksmith vs. Yellow-Pages Locksmith
- **Having newer locks matters**
  - Age makes for a mess, internally
  - Also... your locks should be updated as a matter of routine
- **The facts are out there!**

# So Which Locks are Which ?

- “Unpickable”

-  **ABLOY Protec** (rotating disks)
-  **MCS** (magnetic)
-  **MUL-T-LOCK MT5 and MT5+**
-  **KABAMAS** (electronic safe dial)

- High Security

-  **ABUS** Granit & Diskus (rotating disk)
-  **ASSA** Twin (counter-milling, finger pin)
-  **EVVA** 3KS (sliders), DPI (new mode)
-  **SCHLAGE Primus** (if upgraded properly)

- Resistant

-  **AMERICAN** Padlocks (heavy duty models)
-  **BEST** Interchangeable Cores (modern models)



# Thank you so much.






Thank you to TOOOL, Babak, Dave, Steve, JVR, Mouse, Mr. E, Barry  
& Han, Laz, Valanx & the FOOLS,

Datagram, Matt Blaze, Jackalope, Renderman, Bruce & Heidi, and






# So Which Locks are Which ?

- “Unpickable”

-  **ABLOY** **Protec** (rotating disks)
-  **EVVA** **MCS** (magnetic)
-  **MUL-T-LOCK** **MT5** and **MT5+**
- **KABAMAS** (electronic safe dial)

- High Security

-  **ABUS** Granit & Diskus (rotating disk)
- **ASSA** Twin (counter-milling, finger pin)
-  **EVVA** 3KS (sliders), DPI (new mode)
-  **SCHLAGE** **Primus** (if upgraded properly)

- Resistant

- **AMERICAN** Padlocks (heavy duty models)
- **BEST** Interchangeable Cores (modern models)



<http://deviating.net/lockpicking>

<http://enterthecore.net>

<http://toool.us>